

  
**MITSUBISHI HEAVY INDUSTRIES, LTD.**  
16-5, KONAN 2-CHOME, MINATO-KU  
TOKYO, JAPAN

June 30, 2011

Document Control Desk  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

Attention: Mr. Jeffrey A. Ciocco

Docket No. 52-021  
MHI Ref: UAP-HF- 11201

**Subject: MHI's Responses to US-APWR DCD RAI No.750-5675 Revision 2 (SRP 19)**

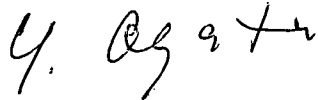
**References:** 1) "Request for Additional Information No. 750-5675 Revision 2, SRP Section: 19 – Probabilistic Risk Assessment and Severe Accident Evaluation," dated April 28, 2011.

With this letter, Mitsubishi Heavy Industries, Ltd. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") a document entitled "Responses to Request for Additional Information No. 750-5675 Revision 2".

Enclosed are the responses to all of the RAIs that are contained within Reference 1.

Please contact Dr. C. Keith Paulson, Senior Technical Manager, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of the submittals. His contact information is below.

Sincerely,



Yoshiki Ogata,  
General Manager- APWR Promoting Department  
Mitsubishi Heavy Industries, LTD.

Enclosure:

1. Responses to Request for Additional Information No. 750-5675 Revision 2

CC: J. A. Ciocco  
C. K. Paulson

Contact Information

C. Keith Paulson, Senior Technical Manager  
Mitsubishi Nuclear Energy Systems, Inc.  
300 Oxford Drive, Suite 301  
Monroeville, PA 15146  
E-mail: ck\_paulson@mnes-us.com  
Telephone: (412) 373-6466

DOB/  
NRW

Enclosure 1

UAP-HF-11201  
Docket Number 52-021

Responses to Request for Additional Information No.750-5675  
Revision 2

June, 2011

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-507**

There is no COL action item in the DCD that addresses generically the issue of updating and upgrading the PRA to meet requirements needed for its intended uses and applications. Instead, a COL action item (COL 19.3(1) in DCD) is identified in the DCD which is specific to risk-managed technical specifications and calls only for updates of the PRA but not upgrades. COL Action Item 19.3(1) must be revised to indicate that it is the responsibility of COL applicants and licensees, as applicable, to update and upgrade the PRA model as necessary to meet the requirements needed for its intended uses and applications and as new or more detailed information becomes available during each of the COL application, construction, and operation phases. Specifically, COL Action Item 19.3(1) must be revised to address the following:

- (a) COL applicants or licensees, as applicable, that reference the US-APWR design will update and upgrade the information in the design-specific PRA to incorporate site-specific and as-built as-operated information per 10 CFR 52.79(d)(1) or 10 CFR 50.71(h)(1).
- (b) PRA will be upgraded before the implementation of risk-informed applications, as necessary, to ensure that asymmetric conditions due to modeling simplicity are eliminated or properly accounted when the PRA results are used for decision making.
- (c) Revised and updated evaluations of the identified operator actions and human error probabilities will be performed as detailed design information becomes available and plant-specific EOPs are developed.
- (d) COL licensees referencing the US-APWR design must develop a PRA maintenance and update program that is consistent with the PRA Standard ASME RA-S-2002 and associated addenda, RG 1.200, and the key elements listed in Section 19.1.2.4 of the DCD.
- (e) It is the responsibility of COL applicants and licensees, as applicable, to update and upgrade the PRA model as necessary to meet the requirements needed for its intended uses and applications and as new or more detailed information becomes available during each of the COL application, construction, and operation phases.
- (f) COL licensees will perform peer reviews of the plant-specific PRA in accordance with

RG 1.200 guidance and will verify that the PRA model is of adequate quality and detail to support the proposed licensee programs and risk-informed applications.

---

**ANSWER:**

DCD Section 19.0 specifies the guidance and standards that were used to develop the DCD PRA model, including ASME/ANS RA-S-2008 and its 2009 addendum (i.e., ASME/ANS RA-Sa-2009). DCD Section 19.1.2.4 "PRA Maintenance and Upgrade," requires that

"In accordance with 10 CFR 50.71(h)(1) (Reference 19.1-15), prior to the scheduled date for initial loading of fuel, a plant-specific PRA that covers initiating events and modes for which NRC-endorsed consensus standards on PRA exist one year prior to the scheduled date for initial loading of fuel will be developed. The plant-specific PRA will reflect the as-built plant. The plant-specific PRA model will utilize the US-APWR DCD PRA model as a baseline. Any additional modeling changes resulting from the plant-specific design, departures from the design used in the US-APWR DCD PRA, insights from procedure development and operator training, or other PRA modeling changes that are identified subsequent to the completion of the US-APWR DCD PRA will also be utilized. The PRA-based risk insight differences between the plant-specific PRA and the US-APWR DCD PRA will be evaluated. Plant walk-downs to confirm that the assumptions used in the PRA remain valid will also be conducted.

During operation, PRA will be maintained and updated in accordance with approved station procedures on a periodic basis not to exceed two refueling cycles.

Changes in PRA inputs or discovery of new information will be evaluated to determine whether the new or changed information warrants a PRA maintenance or upgrade. Changes that would impact risk-informed decisions will be prioritized to ensure that the most significant changes are incorporated as soon as practical. Other changes will be incorporated during the next PRA update.

Changes to the PRA due to PRA maintenance and PRA upgrade will meet the risk assessment technical requirements of the NRC-endorsed PRA standards (Reference 19.1-49 and 19.1-50). Upgrades of the PRA will receive a peer review in accordance with the requirements of the NRC-endorsed PRA standards, but will be limited to aspects of the PRA that have been upgraded.

The PRA will be updated to reflect plant experience, operational experience, and PRA modeling changes, consistent with the NRC-endorsed standards. These standards are described in Section 19.1 and were in existence one year prior to the issuance of the maintenance update scheduled in compliance with 10 CFR 50.71 specified criteria and intervals."

This DCD section also requires that changes to the PRA due to PRA maintenance and PRA upgrade will meet the risk assessment technical requirements of the NRC-endorsed PRA standards, ASME/ANS RA-S-2008 and its 2009 addendum (i.e., ASME/ANS RA-Sa-2009). These standards define, in part, the process for determining when an update or upgrade to the PRA is required (refer to Figure 19.507-1 below).



COL applicants referencing the US-APWR DCD are required to follow the PRA maintenance requirements specified in DCD Sections 19.0 and 19.1. No additional COL item is necessary.

Fig. 1-3-1 Application Process Flowchart

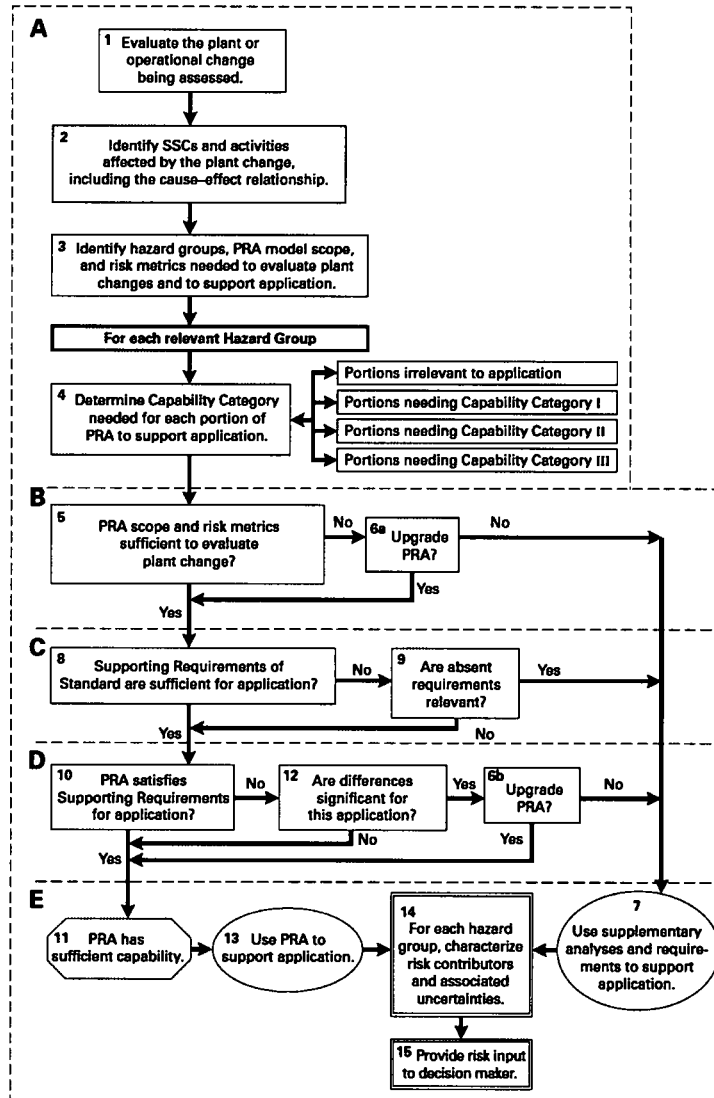


Figure 19.507-1 Application process Flowchart (Ref. ASME/ANS RA-Sa-2009, Figure 1-3-1)

Impact on DCD

There is no impact on the DCD

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-508**

The staff review finds that the current COL action item 19.3(6) must be modified per SRP Chapter 19.0 to address the following:

- Reference to the development and implementation of emergency operating procedures
- Reference to the risk-significant operator actions identified by the PRA and associated assumptions (listed in DCD Table 19.1-119) that a COL applicant/licensee should take into account in the development and implementation of procedures for operation, accident management, training and other human reliability related programs
- Reference to the disposition of risk-significant operator actions discussed in “key insights and assumptions” and/or elsewhere in the DCD
- Ensure that insights gained from the design-specific PRA, including the site and plant-specific information available at the COL application phase, are incorporated in the development of programs and processes which are initiated during or following the COL application phase, such as severe accident management guidelines, emergency operating procedures, reliability assurance, training and human factors engineering.

---

**ANSWER:**

MHI will revise COL Action Item 19.3(6) as follows:

COL 19.3(6) The COL Applicant develops an accident management program which includes emergency operating procedures, [See COL Action Item 13.5(6)] Risk-significant operator actions listed in DCD Table 19.1-119 are to be addressed in the development and implementation of procedures for operation, accident

management, training and other human reliability related severe accident guidance programs. Insights gained from the design-specific PRA, including insights created by the incorporation (unless bounded) of site and plant-specific information available at the COL application phase, are to be reflected appropriately.

DCD Section 19.2.5 will be also revised in accordance with revised COL Action Item 19.3(6), as shown in attached mark-up.

Impact on DCD

Section 19.2.5 and COL Action Item 19.3(6) in DCD Section 19.3.3 will be revised, shown in attached mark-up.

Impact on R-COLA

COL Item 19.3(6) in Table 1.8-201 will be revised, shown in attached mark-up.

Impact on S-COLA

COL Item 19.3(6) in Table 1.8-201 will be revised, shown in attached mark-up.

Impact on PRA

There is no impact on the PRA.

---

guidelines, including Emergency Response Guideline, Severe Accident Management Guidance, etc. Guidance, etc. developed by a COL applicant.

#### Severe Accident Management Framework

The US-APWR applicant develops a severe accident management framework to guide the COL Applicant in the development of plant-specific accident management procedure for the US-APWR design. This accident management procedure discusses the anticipated structure for the decision-making process, the goals to be accomplished in accident management, a summary of possible strategies for the US-APWR accident management, and potential adverse impacts of accident management strategies. A severe accident management guidance includes:

- An approach for evaluating plant conditions and challenges to plant safety functions;
- Operational and phenomenological conditions that may influence the decision to implement a strategy, and which will need to be assessed in the context of the actual event; and
- A basis for prioritizing and selecting appropriate strategies, and approaches for evaluating the effectiveness of the selected actions.

The following countermeasures and operating actions are essentially addressed in the US-APWR severe accident management framework in accordance with the NRC guidance specified in the Reference 19.2-16.

(1) To prevent core damage

(During operations at power)

Key function of accident management to prevent core damage is to keep the core in a condition covered by coolant water. During operations at power, this includes core cooling, secondary cooling, containment cooling, isolation of containment bypass path, power supply, and component cooling. Countermeasures and operator actions for each function are described below.

- Accident management of core cooling function is to prevent core damage in case of LOCA and loss of safety injection. The CS/RHR pump has the function to inject the water from RWSP into the cold leg piping by switching over the CS/RHR pump lines to the cold leg piping (i.e. alternate core cooling operation). If all of safety injection systems are not available, operators are required to switch over the RHRS lines to the cold leg injection.
- Accident management of secondary cooling function is to prevent core damage in case of non-LOCA events. If emergency feedwater pumps cannot feed water to two intact SGs, operators are required to attempt to open the cross tie-line of emergency feedwater pump discharge line in order to feed water to two or more SGs by operable pumps. In case of loss of all feedwater and SG secondary side dried-out, operators are required to initiate the feed and bleed operation by starting the safety injection pump and opening the safety depressurization valve.

---

**19.3 Open, Confirmatory, and COL Action Items Identified as Unresolved**

The following subsections identify the open, confirmatory and COL action items associated with this Chapter.

**19.3.1 Resolution of Open Items**

There are no open items associated with this Chapter.

**19.3.2 Resolution of Confirmatory Items**

There are no confirmatory items associated with this Chapter.

**19.3.3 Resolution of COL Action Items**

The following are the COL action items associated with this Chapter:

COL 19.3(1) The COL Applicant who intends to implement risk-managed technical specifications continues to update Probabilistic Risk Assessment and Severe Accident Evaluation to provide PRA input for risk-managed technical specifications. Peer reviews for the updated PRA will be performed prior to the use of PRA to risk-informed applications.

COL 19.3(2) Deleted

COL 19.3(3) Deleted

COL 19.3(4) The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and associated site-specific external events (high winds and tornadoes, external floods, transportation, and nearby facility accidents).

COL 19.3(5) Deleted

COL 19.3(6) ~~The COL Applicant develops an accident management program which includes severe accident management procedures that capture important operator actions. Training requirements are also included as part of the accident management program.~~

The COL Applicant develops an accident management program which includes emergency operating procedures, [See COL Action Item 13.5(6)] Risk-significant operator actions listed in DCD Table 19.1-119 are to be addressed in the development and implementation of procedures for operation, accident management, training and other human reliability related severe accident guidance programs. Insights gained from the design-specific PRA, including insights created by the incorporation (unless bounded) of site and plant-specific information available at the COL application phase, are to be reflected appropriately.



**Comanche Peak Nuclear Power Plant, Units 3 & 4  
COL Application  
Part 2, FSAR**

CP COL 1.8(2)

**Table 1.8-201 (Sheet 62 of 62)**

**Resolution of Combined License Items for Chapters 1 - 19**

COL Item No.	COL Item	FSAR Location	Resolution Category
COL 19.3(6)	<del>The COL applicant develops an accident management program which includes severe accident management procedures that capture important operator actions. Training requirements are also included as part of the accident management program.</del>	19.2.5	2
	The COL Applicant develops an accident management program which includes emergency operating procedures, [See COL Action Item 13.5(6)] Risk-significant operator actions listed in DCD Table 19.1-119 are to be addressed in the development and implementation of procedures for operation, accident management, training and other human reliability related severe accident guidance programs. Insights gained from the design-specific PRA, including insights created by the incorporation (unless bounded) of site and plant-specific information available at the COL application phase, are to be reflected appropriately.		3a, 3b, 3c, 4, or 5
	3b. Applicant item as Commitment for Design information to be provided before COL issuance		
	3c. Holder item		
	4. Detailed schedule information		
	5. The inspections, tests, analyses, and acceptance criteria (ITAAC) (See Subsection 1.8.1.2 for further discussion.)		

19-508-3

**Table 1.8-201 Resolution of Combined License Items for Chapters 1–19**

COL Item No.	COL Item	FSAR Section	Resolution Category
COL 18.10(2)	Deleted from the DCD.		
COL 18.11(1)	Deleted from the DCD.		
COL 18.11(2)	Deleted from the DCD.		
COL 18.12(1)	Deleted from the DCD.		
COL 19.3(1)	The COL Applicant who intends to implement risk-managed technical specifications continues to update Probabilistic Risk Assessment and Severe Accident Evaluation to provide PRA input for risk-managed technical specifications.	19.1.7.6	NA
COL 19.3(2)	Deleted from the DCD.		
COL 19.3(3)	Deleted from the DCD.		
COL 19.3(4)	The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and associated site-specific external events (high winds and tornadoes, external floods, transportation, and nearby facility accidents).	19.1 19.2	3a
COL 19.3(5)	Deleted from the DCD.		
COL 19.3(6)	<del>The COL applicant develops an accident management program which includes severe accident management procedures that capture important operator actions. Training requirements are also included as part of the accident management program.</del>	19.2.5	2

The COL Applicant develops an accident management program which includes emergency operating procedures, [See COL Action Item 13.5(6)] Risk-significant operator actions listed in DCD Table 19.1-119 are to be addressed in the development and implementation of procedures for operation, accident management, training and other human reliability related severe accident guidance programs. Insights gained from the design-specific PRA, including insights created by the incorporation (unless bounded) of site and plant-specific information available at the COL application phase, are to be reflected appropriately.

19-508-4



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-509**

A new COL action item is needed to ensure that risk insights are used in the development of program and processes and assumptions remain valid. This new COL action item should address the following:

- Ensure that assumptions made about design features and operator actions credited in the PRA should remain valid when the PRA is used to develop such programs and processes.
- Ensure that a COL licensee referencing the certified US-APWR design will review as-designed and as-built information and conduct walk-downs as necessary to confirm that important assumptions made in the PRA about design features and characteristics (e.g., routing and location of piping and cables and HCLPF fragilities) and operator actions remain valid with respect to all applicable events and modes of operation. COL licensees referencing the US-APWR design will perform as-designed and as-built information verification and will conduct walkdowns to confirm that the assumptions used in the PRA remain valid with respect to the internal fire and flood events.
- The design-specific PRA will be updated as necessary when site-specific and plant-specific (as-built) information become available. Differences between the as-built plant and the design used as the basis for the US-APWR PRA will be reviewed to determine whether there is significant impact on PRA results. Special emphasis will be placed on areas of the design that either were not part of the certified design or were not detailed in the certification.

---

**ANSWER:**

As described in DCD Section 17.4, "Reliability Assurance Program," the purposes of the

US-APWR RAP are to provide reasonable assurance that: 1) the US-APWR is designed, constructed, and operated in a manner that is consistent with the assumptions and risk insights for the risk-significant SSCs, 2) the risk-significant SSCs do not degrade to an unacceptable level during plant operations, 3) the frequency of transients that challenge risk-significant SSCs is minimized, and 4) the risk-significant SSCs function reliably when challenged.

DCD Section 17.4.4 describes the controls such as audit plans shall include for consideration, sampling the effectiveness of implementation of RAP implementation procedure. Audits shall consider several key aspects of the RAP including the identification of risk-significant SSCs, whether design and procurement information is consistent with the risk insights from the PRA, and whether assumed equipment reliability is determined to be practicable or achievable.

Additionally, DCD Section 19.1.2.4 "PRA Maintenance and Upgrade," requires that plant walk-downs be conducted to confirm that the assumptions used in the PRA remain valid.

These DCD program commitments, which are incorporated by reference by COL applicants referencing the US-APWR DCD, are adequate to ensure that key insights and features (those identified in the DCD as Table 19.1-119 and as reflected in the incorporation of site specific features and design departures if applicable) are accurately reflected in the design and construction. No new COL item is necessary.

Impact on DCD

There is no impact on the DCD

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-510**

MHI has included several statements in Chapter 19 of the DCD regarding the technical adequacy of the design-specific PRA that are not consistent with RG 1.200. The following statements made in Section 19.1.2 of the US-APWR DCD must be removed or revised. Alternatively, the statements can be revised to state that PRA upgrades should be considered for some future risk-informed applications (e.g., RMTS) and that the entire PRA model, not just the upgrades, will have to receive a peer review in accordance with RG 1.200 requirements:

- "The quality of the PRA is sufficient to provide confidence in the results such that the PRA may be used in regulatory decision-making to support risk-informed applications."
- "The PRA has been developed in accordance with industry consensus standards as described in Section 19.0, and has been subjected to a peer review process as defined in ASME-RA-S-2002 and associated addenda (Reference 19.1-1, 19.1-2, 19.1-3) and as outlined in the Nuclear Energy Institute (NEI) peer review guide (Reference 19.1-14)."
- "Upgrades of the PRA will receive a peer review in accordance with the requirements detailed in Section 6 of ASME-RA-S-2002 and associated addenda, but will be limited to aspects of the PRA that have been upgraded."

---

**ANSWER:**

MHI will remove all of three statements questioned by this RAI.

Impact on DCD

DCD will be revised, shown in attached mark-up.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

---

**19.1.1.4.1 Uses of Probabilistic Risk Assessment in Support of Licensee Programs**

The PRA will be used in the operational phase to support licensee programs such as the human factors engineering program (Chapter 18), the severe accident management program, the maintenance rule, and the reactor oversight program.

**19.1.1.4.2 Risk-Informed Applications**

The PRA will be updated to reflect risk-informed applications during the operational phase.

**19.1.2 Quality of PRA**

The quality of the PRA for the US-APWR is measured in terms of its appropriateness with respect to scope, level of detail, and technical acceptability. RG 1.200 (Reference 19.1-9) was reviewed to ensure that the quality of the US-APWR PRA is consistent with the NRC's expectations. ~~The quality of the PRA is sufficient to provide confidence in the results such that the PRA may be used in regulatory decision making and to support risk informed applications.~~

The following methods are utilized during development of the PRA to ensure that pertinent requirements of 10 CFR 50, Appendix B (Reference 19.1-13) are met:

- Use of qualified personnel
- Use of procedures that ensure control of documentation, including revisions, and provide for independent review, verification, or checking of calculations and information
- Documentation and maintenance of records, including archival documentation, as well as submittal documentation
- Use of procedures that ensure appropriate attention and corrective actions are taken if assumptions, analyses, or information used previously are changed or determined to be in error.

**19.1.2.1 PRA Scope**

The scope of the US-APWR PRA includes a Level 1 and Level 2 PRA for internal and external events (including flooding, fire, and seismic) at full-power, and LPSD conditions.

**19.1.2.2 PRA Level of Detail**

The US-APWR realistically reflects the actual plant design, planned construction, anticipated operational practices, and relevant operational experience. The approach, methods, data, and computer codes that are used, as documented throughout this chapter, are compliant with industry standard codes and practices. The level of detail is sufficient to ensure that the impacts of designed-in dependencies are correctly captured. The level of detail of the PRA is sufficient to provide confidence in the results such that the PRA may be used in regulatory decision-making to support risk-informed applications



in design phase.

### **19.1.2.3 PRA Technical Adequacy**

The quality of the methodologies, processes, analyses, and personnel associated with the US-APWR PRA comply with the provisions for nuclear plant quality assurance. Toward this end, the US-APWR PRA adheres to the recommendations provided in RG 1.200 pertaining to quality and technical adequacy. The US-APWR incorporates the technical elements of an acceptable PRA shown in Table 1 of RG 1.200 (Reference 19.1-9), and is consistent with the technical characteristics and attributes given in Table 2 through Table 10 of RG 1.200. ~~The PRA has been developed in accordance with industry consensus standards as described in Section 19.0, and has been subjected to a peer review process as defined in ASME/ANS RA S-2008 and associated addenda (Reference 10.1 40, 10.1 50) and as outlined in the Nuclear Energy Institute (NEI) peer review guide (Reference 10.1 14).~~

### **19.1.2.4 PRA Maintenance And Upgrade**

The objective of the PRA maintenance and upgrade program is to ensure that the PRA will be maintained and upgraded so that its representation of the as designed, as-to-be built, and as-to-be operated plant is sufficient to support the applications for which the PRA is being used. The PRA will be under configuration control and the program will contain the following key elements:

- A process for monitoring PRA inputs and collecting new information
- A process that maintains and upgrades the PRA to be consistent with the as-built, as-operated plant
- A process that ensures the cumulative impact of pending changes is considered when applying the PRA
- A process that evaluates the impact of changes on previously implemented risk-informed decisions that have used the PRA
- A process that maintains configuration control of computer codes used to support PRA quantification
- Documentation of the program

PRA maintenance involves updating of PRA models to reflect plant changes such as modifications, procedure changes, or plant performance. A PRA upgrade involves the incorporation into the PRA model of new methodologies or significant changes in scope or capability. Those changes could include items such as new human error analysis methodology; new data update methods; new approaches to quantification or truncation; or new treatments of common cause failure (CCF).

In accordance with 10 CFR 50.71(h)(1) (Reference 19.1-15), prior to the scheduled date for initial loading of fuel, a plant-specific PRA that covers initiating events and modes for which NRC-endorsed consensus standards on PRA exist one year prior to the scheduled date for initial loading of fuel will be developed. The plant-specific PRA will reflect the

as-built plant. The plant-specific PRA model will utilize the US-APWR DCD PRA model as a baseline. Any additional modeling changes resulting from the plant-specific design, departures from the design used in the US-APWR DCD PRA, insights from procedure development and operator training, or other PRA modeling changes that are identified subsequent to the completion of the US-APWR DCD PRA will also be utilized. The PRA-based risk insight differences between the plant-specific PRA and the US-APWR DCD PRA will be evaluated. Plant walk-downs to confirm that the assumptions used in the PRA remain valid will also be conducted.

During operation, PRA will be maintained and updated in accordance with approved station procedures on a periodic basis not to exceed two refueling cycles.

Changes in PRA inputs or discovery of new information will be evaluated to determine whether the new or changed information warrants a PRA maintenance or upgrade. Changes that would impact risk-informed decisions will be prioritized to ensure that the most significant changes are incorporated as soon as practical. Other changes will be incorporated during the next PRA update.

Changes to the PRA due to PRA maintenance and PRA upgrade will meet the risk assessment technical requirements of the NRC-endorsed PRA standards (Reference 19.1-49 and 19.1-50). ~~Upgrades of the PRA will receive a peer review in accordance with the requirements of the NRC endorsed PRA standards, but will be limited to aspects of the PRA that have been upgraded.~~

The PRA will be updated to reflect plant experience, operational experience, and PRA modeling changes, consistent with the NRC-endorsed standards. These standards are described in Section 19.1 and were in existence one year prior to the issuance of the maintenance update scheduled in compliance with 10 CFR 50.71 specified criteria and intervals.

### **19.1.3 Special Design/Operational Features**

Design and operational features of the US-APWR that result in improved plant safety as compared to currently operating nuclear power plants, include the following:

- Mechanical four train systems with direct vessel injection (DVI) system design
- Elimination of the need for low-head safety injection (LHSI) pumps by utilizing an advanced accumulator injection system
- Elimination of recirculation switching by an in-containment RWSP
- Enhanced safety through the use of four trains of safety electrical systems
- Upgraded piping design pressure for the residual heat removal system (RHRS)

The major unique features of the US-APWR related to PRA scope are

- Four train core cooling - High reliability due to four advanced accumulators and a four train high head injection system



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-511**

MHI must perform a systematic search to identify "key sources of uncertainty" from all PRA areas and list them in the DCD as part of the risk insights required by the design certification process and to ensure that uncertainties are addressed in future PRA applications. In addition, MHI should include in the DCD the following identified (in RAI responses) key sources of uncertainty:

1. CCF probability of CCW and ESW pumps
  2. Unavailability due to maintenance of CCW pumps, ESW pumps, and other risk-important components
  3. Failure probability of risk-important components with long testing intervals
  4. Modeling of the PSVs in the PRA due to maintenance of CCW pumps, ESW pumps, and other risk-important components
  5. Modeling of the CCF of I&C hardware and associated probability
  6. CCF probability of basic software
  7. CCF probability of support software
- 

**ANSWER:**

MHI performed a systematic search to identify key sources of uncertainty from PRA areas and inserted the identified key sources and their impact on PRA in the US-APWR DCD Rev.3 Tables 19.1-38 and 19.1-140, respectively. Key sources of uncertainty are identified in the following manner. US-APWR PRA uses the various assumptions to unreliability of unique designs such as advanced accumulators, gas turbine generators, DAS or digital I&C system, component configuration related to test and maintenance, operator actions such as frequent training. Running or standby trains in CCWS and ESWS are also assumed in accordance with design information. The assumptions are decided to become more conservative. The assumptions used in the PRA have large uncertainty and may have large impact on PRA



results. DCD Table 19.1-38 summarizes the key sources of uncertainty that may have impact on PRA results. For the assumptions, not only uncertainty analysis but sensitivity analyses assuming various unreliabilities were performed to clarify the contribution to the risk. The results have been summarized in DCD Table 19.1-140.

Within the seven items requested by this RAI Question, Items 1, 2, 3 and 5 have been incorporated in Table 19.1-38. The other items discussed below will be inserted in the DCD

#### Item 4: Modeling of the PSVs

US-APWR has four PSVs to prevent the overpressure of RCS. Loss of offsite power (LOOP), loss of CCW (LOCCW) or partial loss of CCW (PLOCW) event results in RCS pressurization, and then the PSVs automatically open. If at least one of PSVs fails to re-close after their opening, LOCA event occurs, i.e., safety valve stuck open LOCA. There is an uncertainty that RCS pressure exceeds PSV set pressure following these initiating events. PRA conservatively assumes that the RCS pressure will always exceed the operating pressure of PSV and failure of PSV to reclose will result in safety valve stuck open LOCA.

Estimated CDF assuming that RCS pressure does not always exceed the PSV set pressure following LOOP, LOCCW or PLOCW event is  $1.0E-06/RY$ , which is less than 1% of the base case CDF. Uncertainty related to the PSV assumption has sufficiently small impact on risk.

#### Item 6: CCF probability of basic software

US-APWR uses the common basic software for safety-related (PSMS) and non-safety related (PCMS) I&C system, excluding AAC. Basic software CCF will result in failure of all automatic signals and operator action using I&C system besides AAC start signal.

The base case assumes that basic software CCF probability is  $1.0E-07/demand$ . Since this probability has high uncertainty, sensitivity analyses concerning basic software CCF are performed to study the uncertainty.

##### Case 1: Basic software CCF = $2.0E-07/demand$

If basic software CCFs are assumed to occur  $2.0E-07/demand$ , which is twice the value considered in the base case, the resulting CDF is  $1.0E-06/RY$ . This value is 0.5% higher than the base case CDF.

##### Case 2: Basic software CCF = $5.0E-07/demand$

If basic software CCFs are assumed to occur  $5.0E-07/demand$ , the CDF is estimated to be  $1.0E-06/RY$ , which is 1.9% higher than the base case CDF.

##### Case 3: Basic software CCF = $1.0E-06/demand$

If basic software CCFs are assumed to occur  $1.0E-06/demand$ , the resulting CDF is  $1.1E-06/RY$ . This value is 4.3% higher than the base case CDF.

The above results show that if the probability of basic software CCF, which causes failure of all automatic signals and operator actions using PSMS and PCMS, occurs with ten times probability of base case, the resulting CDF is  $1.1E-06/RY$ . The result is approximately 5% higher than the base case CDF.

#### Item 7: CCF probability of hardware

US-APWR adopts the common hardware for PSMS. I&C hardware CCF will result in failure of all automatic signals and operator action using PSMS.

The base case assumes that I&C hardware CCF of safety-related I&C system (i.e., PSMS) is  $1.0E-07/\text{demand}$ . Since this probability has high uncertainty, sensitivity analyses concerning I&C hardware CCF are performed to study the uncertainty.

Case 1: Hardware CCF =  $5.0E-06/\text{demand}$

If hardware CCFs are assumed to occur  $5.0E-06/\text{demand}$ , the resulting CDF is  $1.1E-06/\text{RY}$ . This value is 4.4% higher than the base case CDF.

Case 2: Hardware CCF =  $1.0E-05/\text{demand}$

If hardware CCFs are assumed to occur  $1.0E-05/\text{demand}$ , the CDF is estimated to be  $1.1E-06/\text{RY}$ , which is 11% higher than the base case CDF.

Case 3: Hardware CCF =  $2.1E-05/\text{demand}$

If hardware CCFs are assumed to occur  $2.1E-05/\text{demand}$ , which is ten times of base case, the resulting CDF is  $1.3E-06/\text{RY}$ . This value is 27% higher than the base case CDF.

Results of sensitivity analyses show that if the probability of I&C hardware CCF, which results in failure of all automatic signals and operator action using PSMS, occurs with a probability of  $2.1E-05/\text{demand}$ , the resulting CDF is  $1.3E-06/\text{RY}$ . The result is approximately 1.3 times of the base case CDF.

#### Impact on DCD

DCD will be revised, shown in attached mark-up.

#### Impact on R-COLA

There is no impact on the R-COLA.

#### Impact on S-COLA

There is no impact on the S-COLA.

#### Impact on PRA

There is no impact on the PRA.

Standard Technical Specification (STS) (Reference 19.1-51, 19.1-52). TS requirements have influence on the unavailability of each equipments and modules that constitute the PSMS and hence influence the PRA results. Sensitivity analyses have been performed to evaluate the changes in CDF associated with the variables of TS requirements regarding PSMS. If the STS requirements were to be applied for the PSMS, the CDF from internal events would be  $9.9E-07/RY$ . Changes of TS requirements for PSMS and reactor trip system from the STS to the current US-APWR TS results in  $3.2E-08/RY$  increase to the internal events CDF, which is approximately a 3% increase. TS changes have only a small impact on risk.

- CASE 4-3: Common cause failure of application software between safety related signals and AAC

US-APWR is designed to minimized common cause failure between Class 1E GTGs and non-Class 1E GTGs (i.e., AACs) . In this sensitivity analysis, common application software is used for both Class 1E GTGs and AACs. The CDF is  $1.5E-06/RY$ , which is 48% higher than the base case CDF. The characteristic design for US-APWR is effective to reduce risk depending on the power supply in LOOP event.

Design and operation

Sensitivity analysis of design and operation is performed to study the impact of key design and operation on plant CDF for internal initiating events at power.

- CASE 5-1: Emergency feedwater pit capacity

If each EFW pit, which has 50% capacity to perform cold shutdown, is enlarged to have 100% capacity to perform cold shutdown, the CDF will be  $9.6E-07/RY$ . This CDF is 6% lower than the base case CDF.

- CASE 5-2: Operation of emergency feedwater pump discharge line cross tie-line valves

If the emergency feedwater pump discharge line cross tie-line valves, which are opened when emergency feedwater pumps fail to supply at least two SGs, are kept closed regardless of emergency feedwater pump failures, the CDF will be  $1.8E-06/RY$ . This CDF is 77% higher than the base case CDF.

- CASE 5-3: Common mode failure of all sump screens

In the base case, common cause failure of sump screens are evaluated from with generic failure data and generic common cause failure parameters. Although sump screens of US-APWR are design to minimize failure due to clogging, common cause failure CCF probability of sump screen may increase at for large LOCA. In this sensitivity analysis, the probability of all four sump screens to clog at large LOCA has been assumed to be  $0.0625 (=0.5^4)$  per demand. The resulting CDF is  $1.1E-06/RY$ . This CDF is 8% higher than the base case CDF.

Insert A  
in next page

## Insert A

- CASE 4-4: Common cause failure of basic software

The base case assumes that basic software CCF probability is  $1.0E-07/\text{demand}$ . Since this probability has high uncertainty, sensitivity analyses concerning basic software CCF are performed to study the uncertainty.

Case 1: Basic software CCF =  $2.0E-07/\text{demand}$

If basic software CCFs are assumed to occur  $2.0E-07/\text{demand}$ , which is twice the value considered in the base case, the resulting CDF is  $1.0E-06/\text{RY}$ . This value is 0.5% higher than the base case CDF.

Case 2: Basic software CCF =  $5.0E-07/\text{demand}$

If basic software CCFs are assumed to occur  $5.0E-07/\text{demand}$ , the CDF is estimated to be  $1.0E-06/\text{RY}$ , which is 1.9% higher than the base case CDF.

Case 3: Basic software CCF =  $1.0E-06/\text{demand}$

If basic software CCFs are assumed to occur  $1.0E-06/\text{demand}$ , the resulting CDF is  $1.1E-06/\text{RY}$ . This value is 4.3% higher than the base case CDF.

The above results show that if the probability of basic software CCF, which causes failure of all automatic signals and operator actions using PSMS and PCMS, occurs with ten times probability of base case, the resulting CDF is  $1.1E-06/\text{RY}$ . The result is approximately 5% higher than the base case CDF.

- CASE 4-5: Common cause failure of hardware

The base case assumes that I&C hardware CCF of safety-related I&C system (i.e., PSMS) is  $1.0E-07/\text{demand}$ . Since this probability has high uncertainty, sensitivity analyses concerning I&C hardware CCF are performed to study the uncertainty.

Case 1: Hardware CCF =  $5.0E-06/\text{demand}$

If hardware CCFs are assumed to occur  $5.0E-06/\text{demand}$ , the resulting CDF is  $1.1E-06/\text{RY}$ . This value is 4.4% higher than the base case CDF.

Case 2: Hardware CCF =  $1.0E-05/\text{demand}$

## Insert A

If hardware CCFs are assumed to occur  $1.0\text{E-}05/\text{demand}$ , the CDF is estimated to be  $1.1\text{E-}06/\text{RY}$ , which is 11% higher than the base case CDF.

Case 3: Hardware CCF =  $2.1\text{E-}05/\text{demand}$

If hardware CCFs are assumed to occur  $2.1\text{E-}05/\text{demand}$ , which is ten times of base case, the resulting CDF is  $1.3\text{E-}06/\text{RY}$ . This value is 27% higher than the base case CDF.

Results of sensitivity analyses show that if the probability of I&C hardware CCF, which results in failure of all automatic signals and operator action using PSMS, occurs with a probability of  $2.1\text{E-}05/\text{demand}$ , the resulting CDF is  $1.3\text{E-}06/\text{RY}$ . The result is approximately 1.3 times of the base case CDF.



S The CDF assuming the RCS pressure does not exceed the pressurizer safety valve set pressure is estimated to be  $1.0E-06/RY$ , which is less than 1% of base case CDF.

In the base case, pressurizer safety valves are assumed to be open following an initiating event such as LOOP, LOCCW or PLOCW and failure of at least one of the valves to re-close leads to stuck open safety valve LOCA. ~~In sensitivity analysis, the valve is automatically opened when the RCS pressure is above the valve set pressure and failure of the valves to re-close results in the stuck open safety valve LOCA. Then, the CDF is  $1.4E-06/RY$ , which is 33% higher than the base case.~~

After LOOP event, the reactor will be instantly tripped due to loss of power supply to the reactor trip breakers. Since pressurizer safety valve set pressure, the assumption has sufficiently small impact on CDF. Although the RCS pressure is unlikely to reach the pressurizer safety valve set pressure, the assumption has sufficiently small impact on CDF.

~~operators will detect the symptom of the event, such as low pressure at pump outlet or high CCW temperature and manually trip the plant before losses of main feedwater would occur. In most cases, the reactor would be tripped before SG cooling ability degrades. The RCS pressure is unlikely to reach the pressurizer safety valve set pressure. Therefore, the assumption that failure of the valve to open or re-close leads to stuck open safety valve LOCA is conservative.~~

Valve Reliability

Sensitivity analysis of valve reliability that has high FV importance and long test interval is performed to study the impact of its uncertainty on plant CDF for internal initiating events at power.

- CASE 7-1: Test Interval of Valves

Failure probabilities of valves used in the US-APWR PRA are independent from their test intervals. The failure probability of valves reported in NUREG/CR-6928 is based on failure data of valves that have average test intervals less than 12 months. Sensitivity analyses are performed applying higher failure probabilities to valves that have FV importance higher than  $2.0E-03$ , considering longer test intervals based on inservice testing (IST) requirements (e.g., 24 months). Valves that have high FV importance and have test intervals sufficiently longer than the NUREG data are the followings.

- Main steam isolation valves (MSS-SMV-515A, B, C, D)
- EFW pit outlet check valves (EFS-VLV-008A, B)
- EFW pump outlet check valves (EFS-VLV-012A, B, C, D)
- EFW line check valves (EFS-VLV-018A, B, C, D)
- Safety depressurization valves (RCS-MOV-117A, B)
- Pressurizer safety valves (RCS-SRV-120, 121, 122, 123)

All of these valves are under control of the in-service test program and are required to be tested every 24 months except the pressure safety valves, which is tested every 60 months. Demand failure probabilities of NUREG/CR-6928 are



A PRA study involves many sources and types of uncertainty. Some are quantifiable and can be propagated through the model to generate an uncertainty distribution. Others deal with issues such as the state of knowledge and are difficult to quantify. Key sources of uncertainty and key assumptions made in the development of the PRA model for internal events at power are provided in next. They are identified and assessed for their impact on the results of the PRA.

The assessed areas of uncertainty include parametric uncertainty, modeling uncertainty, and completeness uncertainty.

Parametric uncertainty involves gathering information on the uncertainty associated with parametric values and propagating these through modeling formalisms. This process results in a better understanding of the variability of the mean or expected value of the distribution and the range of outcomes possible. A parametric uncertainty evaluation has been performed that propagates the uncertainty distribution through the model to produce the mean value of CDF using Monte Carlo simulation.

The result of the parametric uncertainty evaluation is shown in Figure 19.1-5. The mean, median, low and high values of the distribution are calculated. The error ratio of the 95th percentile to the 5th percentile is 3.0.

US-APWR PRA uses the various assumptions to unavailability of unique design such as advanced accumulators, GTGs or digital I&C system, component configuration related to test and maintenance, human actions such as training and initial condition (e.g., running or standby train) assumed in PRA. The assumptions that have large uncertainty are summarized in Table 19.1-38.

The plant CDF uncertainty range is found to be  $2.9E-06/RY - 3.1E-07/RY$  for the 95% to 5% interval. This indicates that there is 95% confidence that the plant CDF is no greater than  $2.9E-06/RY$ . The EF for the total CDF is 3.0.

Modeling uncertainty involves key assumptions and key decisions made in developing the model. Table 19.1-38 lists key sources of uncertainty and key assumptions made in the development of the PRA model along with a qualitative assessment of the items pertaining to modeling uncertainty. Table 19.1-140 summarizes the PRA impact associated with key sources of uncertainty and key assumptions in the PRA model development.

Completeness uncertainty is associated with the possibility of unaccounted for initiating events. Extensive effort has been put forth to identify a comprehensive set of initiating events, yet it is recognized that rare events may arise which cause plant response. Such events may not be adequately captured in the database as failure mechanisms may not be known and conditions in which they might arise have not occurred. Rare initiating events are considered in this study even if they have not occurred yet.

The insights from PRA results are following:

- The CDF for operations at power is  $1.0E-06/RY$  which is less than that PWRs currently operating. The design features of US-APWR such as the four train safety system, independent four train electrical system, in-containment RWSP and alternate ac power source reduce the risk of core damage.
- The conditional CDF under conditions where one safety system train is out of service is below  $1.0E-05/RY$ . Highly redundant safety system enables to maintain CDF below considerable value even when one train is out of service.

Table 19.1-38 Key Sources of Uncertainty and Key Assumptions (Level 1 PRA for Internal Events at Power)  
(Sheet 5 of 9)

Key Sources of Uncertainty and Key Assumptions		Type (Note)	Summary Results of Qualitative Assessments	Quantitative Approach
System Analysis	Outage types and their frequencies	M	The four train safety system design of the US-APWR gives higher flexibility of maintenance compared to conventional plants. It is expected that this design feature will reduce the frequency of unplanned shutdown. However, there are uncertainties associated with the frequencies of unplanned shutdown and their duration. A sensitivity analysis which considers the shutdown frequency of all outage types was performed. <b>LOCCW, LOCW or LOOP</b>	Sensitivity Analysis (Case 04 LPSP)
	Status of pressurize safety valves	M	In <del>LOCCW or LOOP</del> event, initial state of pressurizer safety valves is assumed to be kept open. Then, one of the valves fails to re-close, resulting in LOCA (i.e., safety valve stuck open LOCA). Sensitivity analysis assuming that <del>the valves are initially closed</del> was performed. <b>RCS pressure would not exceed set value of pressurizer safety valve following the initiating events</b>	Sensitivity Analysis (Case <del>5-4</del> ) <b>6-1</b>
Data Analysis	Test interval of equipments	M	Test the same as the Standard IS. Sensitivity analysis of valve reliability that has high FV importance and long test interval (24 months or more) was performed.	Sensitivity Analysis (Case <del>6-4</del> ) <b>7-1</b>



Table 19.1-38 Key Sources of Uncertainty and Key Assumptions (Level 1 PRA for Internal Events at Power)  
(Sheet 6 of 9)

Key Sources of Uncertainty and Key Assumptions		Type (Note)	Summary Results of Qualitative Assessments	Quantitative Approach
Data Analysis	Applicability of failure modes to the US-APWR equipment design	M	Potentially valuable generic data sources were collected. All the failure modes of the US-APWR component types were considered.	NA
	Failure probability and failure rates for diesel generators are applied to gas turbine generators.	M	<del>Sensitivity analysis of failure probability and failure rates was performed.</del>	Sensitivity Analysis (Case 3-2)
	Statistical uncertainty of failure rate	P	(Statistical uncertainty is considered)	Uncertainty Analysis
	Failure probability of digital I&C software	M	Sensitivity analysis of failure probability was performed.	Sensitivity Analysis (Case 4-4)
	Reliability of components	M	There is no plant-specific reliability data for the US-APWR. In the design stage, it is likely that the reliability of components of a newly designed plant is within the range of operating US plants. Therefore, US generic data is applicable.	4-1, 4-4, 4-5 NA

Sensitivity analyses of various failure probability were performed

Table 19.1-140 Impact on PRA Association  
(Level 1 PRA for Int

Key Sources of Uncertainty and Key Assumptions		Sensitivity Analysis Case	
Unique Equipments and their Duty to the US-APWR Design	Gas turbine generators	Case 3-2	<p>When the probability of application software CCF or basic software CCF results in failures of all automatic signals and operator action using I&amp;C system is set to ten times the base case, the CDF is 1.3 times higher than base case.</p> <p>CDF assuming probability of hardware CCF with ten times of base case, which causes failure of PSMS, is 1.3 times of base case CDF. the results show the uncertainty of I&amp;C system is small impact on CDF.</p> <p>case. Failure data of GTGs has uncertainty of CDF.</p>
	Digital I&C	Case 4-1 4-1, 4-4, 4-5	<p><del>When the failure probability of application software CCF that results in failures of safety related signals and operator actions is set to ten times of base case, the CDF is 1.3 times higher than base case. This shows the uncertainty of application software CCF is small impact on CDF.</del></p>
	AAC application software	Case 4-3	<p>I&amp;C system for AACs is designed to be independent from software for safety-related equipment such as Class 1E GTGs. The CDF is 1.5E-06/Ry, which is approximately 50% higher than base case. The characteristic design of US-APWR enables to reduce risk during plant operation.</p>
System Analysis	System unavailability due to test and maintenance	Case 1-1, 1-2, 1-3, 1-4	<p>The CDF is 4.4E-06/Ry when one safety train is out of service all year. Four train safety systems of US-APWR design enable to reduce risk caused by on power maintenance during at-power operation.</p>



19. PROBABILISTIC RISK ASSESSMENT  
AND SEVERE ACCIDENT EVALUATION

US-APWR Design Control Document

Key Sources of Uncertainty and Key Assumptions		Sensitivity Analysis Case	
<p><b>Table 19.1-140 Impact on PRA Associated with Pressurizer Safety Valve Stuck Open (Level 1 PRA for Intermittent Pressurizer Safety Valve Stuck Open)</b></p>			<p>The increased CDF assuming the RCS pressure does not exceed the pressurizer safety valve set pressure following an initiating event such as LOOP, LOCCW or PLOCW is less than 1% of the base case CDF. Uncertainty on the RCS pressurization that may cause safety valve stuck open LOCA has small impact on CDF.</p>
System Analysis	Status of pressurize safety valves	<p>Case 5-4 6-1</p>	<p><del>The CDF assuming the RCS pressure always exceeds the set pressure after initiating event such as LOOP or LOCCW is 1.4E-06/RY. Considering possibility that the pressure exceeds the set pressure, the assumption that the valves are always kept open, which is used in base case, is negligible.</del></p>
Data Analysis	Test interval of equipments	<p>Case 6-1 7-1</p>	<p>In the sensitivity analysis with longer test interval for valves, the maximum CDF is 1.2E-06/RY. Most equipments are controlled by TS in Chapter 16, and the uncertainty associated with test interval has small impact.</p>
	Failure probability and failure rates for diesel generators are applied to gas turbine generators.	Case 3-2	<p>In the base case, failure data of diesel generators are applied to GTGs. In the sensitivity analysis, the failure data of gas turbine generators are applied and then, the increase of CDF is approximately 30% from the base case. Failure data of GTGs has uncertainty of CDF.</p>
	Failure probability of digital I&C software	Case 4-1	<p>When the failure probability of application software CCF that results in failures of safety related signals and operator actions is set to ten times of base case, the CDF is 1.3 times higher than base case. This shows the uncertainty of application software CCF is negligible.</p>
Common Cause Failure Analysis	CCF parameters of emergency diesel generators are applied to gas turbine generators.	Case 3-1	<p>In base case, CCF parameters for diesel generators are applied to gas turbine generators. In the sensitivity analysis case, the CCF parameters for general components, which is smaller than the diesel generators, are applied. The CDF is 7.8E-07/RY, which is 24% lower than the base case. The results shows the GTGs have impact on uncertainty of CDF.</p>

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-512**

Based on SRP 19.0, the staff review finds that MHI must perform a systematic search to identify "key insights and assumptions" regarding design and operational features which must be included in the DCD (e.g., revise existing Table 19.1-119) with a proper disposition which ensures that these "assumptions" will remain valid in the as-to-be-built, as-to-be-operated plant. In addition, MHI must include in the DCD "key insights and assumptions," with a proper disposition, that have been identified in responses to staff RAIs related to the following items:

1. Design and operational features that prevent interfacing systems LOCA.
2. Design and operational features that prevent intersystem CCF of check valves in the injection lines, such as: (a) different driving forces applied to the passive accumulators from the driving forces of pumps that are present in the HHI and CS/RHR systems; (b) different system testing cycles; and (c) different maintenance practices.
3. Assumptions made regarding hardware and software diversity must be stated clearly along with their basis and an appropriate disposition.
4. The assumption to install a diverse non-safety related EFW pit water level sensor.
5. Design and operational features identified in the responses to RAI Questions 19-275 and 19-383.
6. The basis for not modeling the loss of HVAC in the ESF area, where HHI and CS/RHR pumps are located.
7. The presence of interlocks, implemented on the EFW control valves and EFW isolation valves, which ensures that the SG water level is within the range for effective secondary cooling regardless of operator action.
8. The PRA assumption that the availability and reliability of all trains of safety-related systems will be controlled by the maintenance rule and configuration risk management programs, including the setting of availability goals for each one of the four trains, the tracking of availability, and comparison to the set goals.
9. The means for controlling the availability of the reactor trip and ESF actuation function of DAS.

---

**ANSWER:**

MHI performed a systematic search to identify key insights and assumptions regarding US-APWR design and operational features and summarized them in Table 19.1-119 of the US-APWR DCD Rev.3.

Within the nine items requested by this RAI question, Items 1, 2, 4, 8 and 9 have already been listed in Table 19.1-119. The other items will be incorporated in Table 19.1-119. Then, for Items 5 and 6, the response to RAI Question 19-516 provides the room temperature analysis results to demonstrate that SI, CS/RHR and T/D EFW pumps can be operable without room cooling. Also, MHI performed sensitivity analysis assuming no restoration of HVAC system within mission time, resulting in no SI pumps, CS/RHR pumps, T/D and M/D EFW pumps. The resulting CDF is  $3.8E-05/R$ , which is approximately 40 times of the base case CDF. CCF of the HVAC system will result in failure of core injection system by SI pumps or CS/RHR pumps and secondary side cooling system via SGs. The US-APWR design that safety-related components such as SI pumps, CS/RHR pumps or EFW pumps can operate without room cooling within mission time is important to reduce CDF. A new table which summarizes the room temperature analysis results will be placed as the DCD Table 19.1-180 and be referenced in a disposition of each element in the DCD Table 19.1-119.

Impact on DCD

Table 19.1-119 will be revised, shown in attached mark-up..

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

**Table 19.1-119 Key Insights and Assumptions (Sheet 1 of 46)**

Key Insights and Assumptions	Dispositions
<b>Design features and insights</b>	
1. High Head Safety Injection System	
- The high head safety injection system consists of four independent and dedicated SI pump trains.	6.3.2.1.1
- The SI pump trains are automatically initiated by ECCS actuation signal, and supply borated water from the RWSP to the reactor vessel via direct vessel injection line.	6.3.2.1.1
- Each SI pump is connected to a dedicated direct vessel injection nozzle for injection into the reactor downcomer region.	6.3.2.1.1
- SI pump suction isolation valves (SIS-MOV-001A/B/C/D) remain open during normal and emergency operations. These valves are remotely closed by operator action from MCR or RSC to isolate RWSP to terminate leak or if pump/valve maintenance requires it.	6.3.2.2.6.1
- This system provides the safety injection function during LOCA events and feed and bleed operation.	6.3.3 19.2.5 COL13.5(6) COL19.3(6)
- During plant shutdown, safety injection provides RCS makeup function in loss of RHRS. In the case of failure of operable SI pump, the pumps that are locked out for LTOP compliance can be used if available.	5.2.2.1.2 5.2.2.2.2 19.2.5 COL13.5(6) COL19.3(6)
- SI pump can be manually actuated by DAS from MCR.	7.8.1.1.1 Table 7.8-5
- SI pumps are operable regardless of HVAC system of the safeguard component area within mission time.	Table 19.1-180



**Table 19.1-119 Key Insights and Assumptions (Sheet 5 of 46)**

Key Insights and Assumptions	Dispositions
<ul style="list-style-type: none"> <li>- The RHR system is used to provide core cooling when the RCS must be partially drained to allow maintenance or inspection of the reactor head, SGs, or reactor coolant pump seals.</li> </ul>	5.4.7.2.3.6
<ul style="list-style-type: none"> <li>- When the RCS temperature and pressure are reduced to 350°F and 400 psig, the RHRS provides the heat removal function.</li> </ul>	5.4.7.2.3.3 19.1.6
<ul style="list-style-type: none"> <li>- During mid-loop operation, low-pressure letdown line isolation valves, which are air-operated valves, are automatically closed to isolate CVCS from RHRS by detection of RCS loop low-level signal. This interlock is useful to prevent loss of reactor coolant inventory.</li> </ul>	5.4.7.2.2.3 5.4.7.2.3.6 7.6.1.7 TS 3.4.8 TS 3.9.6
<ul style="list-style-type: none"> <li>- The containment spray/residual heat removal pump full-flow test line stop valves (RHS-MOV-025A/B/C/D) are locked closed.</li> </ul>	5.4.7.2.2.3

<ul style="list-style-type: none"> <li>- CS/RHR pumps are operable regardless of HVAC system of the safeguard component area within mission time.</li> </ul>	Table 19.1-180
--	----------------

Table 19.1-119 Key Insights and Assumptions (Sheet 10 of 46)

Key Insights and Assumptions	Dispositions
<p>9. Emergency Feedwater System</p> <ul style="list-style-type: none"> <li data-bbox="409 410 1197 534">- EFWS, which consists of two motor-driven pumps and two steam turbine-driven pumps with two emergency feedwater pits, is designed to remove decay heat through the SGs following transient conditions or postulated accidents.</li> <li data-bbox="409 559 1197 651">- The EFWS supply feedwater to the SGs whenever RCS temperature above 350°F and the main feedwater system is not in operation.</li> <li data-bbox="409 676 1197 768">- The EFWS is designed with two 50% EFW pits, both pits together provide a sufficient volume of water required for the emergency condition.</li> <li data-bbox="409 793 1197 1008">- Each EFW pump discharge line connects with a tie line with a motor-operated isolation valve. During normal plant operation (at non-OLM), the discharge tie line isolation valves of each EFW pump discharge tie line are in the closed position to provide separation of four trains. During OLM, the tie line isolation valves of each EFW pump discharge tie line are kept in the open position.</li> <li data-bbox="409 1034 1197 1125">- Upon detection of a water level increase of the SG, the EFW isolation valves and EFW control valves are automatically closed.</li> <li data-bbox="409 1151 1197 1242">- The motor-operated EFW isolation valves and EFW control valves are provided in each EFW pump discharge line to close automatically to terminate the flow to the affected SG.</li> <li data-bbox="409 1268 1197 1449">- The common suction line from each EFW pit is connected by a tie line with two normally closed manual valves. When the two EFW pumps taking suction from the same pit are not available (OLM of one EFW pump and the single failure of other EFW pump), the tie line connections to EFW pits need to be established.</li> <li data-bbox="409 1474 1197 1566">- The demineralized water storage tank provides a backup source for EFWS. The manual valves from the demineralized water storage tank to the EFW pumps are normally closed.</li> <li data-bbox="409 1591 1197 1821">- To cope with common cause failure of EFW pit water level sensors, a non-safety water level sensor diverse from the safety related water level sensors are installed in each EFW pit. Low water level in the EFW pit can be detected by these non-safety sensors. Accordingly, the operator can recognize the low water level in the EFW pit during EFW pump operation with high reliability.</li> </ul>	<p>10.4.9 10.4.9.1 10.4.9.2</p> <p>10.4.9</p> <p>10.4.9.2 10.4.9.2.1</p> <p>10.4.9.2 10.4.9.2.1</p> <p>10.4.9.2 7.3.1.5.10 Table 7.3-3</p> <p>10.4.9.2</p> <p>10.4.9.2</p> <p>10.4.9.2.1</p> <p>10.4.9.2.4</p>



Table 19.1-119 Key Insights and Assumptions (Sheet 11 of 46)

Key Insights and Assumptions	Dispositions
<ul style="list-style-type: none"> <li>- The EFWS is automatically initiated by EFW actuation signal or by DAS.</li> </ul>	7.3.1.5.9 7.8.1.2.2 Table 7.8-5 10.4.9.1
<ul style="list-style-type: none"> <li>- The EFWS design is provided with the capability to automatically terminate EFW flow to a depressurized (faulty) SG and to automatically provide EFW to the intact SGs.</li> </ul>	7.2.1.5.10 10.4.9.1 10.4.9.2 10.4.9.2.1
<ul style="list-style-type: none"> <li>- The system supplies feedwater to the SGs at a sufficient flow rate to meet the requirements for the transient conditions or postulated accidents and hot standby.</li> </ul>	10.4.9
<ul style="list-style-type: none"> <li>- Motor-driven EFW pumps require room cooling for operation. On the other hand, turbine-driven EFW pumps are operable regardless of the <del>availability</del> of room cooling.</li> </ul>	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Table 19.1-180</div>

<ul style="list-style-type: none"> <li>- The EFWS is automatically initiated by the receipt of the EFW actuation signal such as the low SG water level signal</li> </ul>	10.4.9.1 10.4.9.2.1 7.3.1.5.9 Table 7.3-3
--	--

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-513**

The staff requested additional information (RAI Questions 19-97, 19-98 and 19-364) regarding the implementation of the approach that was followed to determine PRA success criteria. In some cases, credit is taken in the T-H analysis of “bounding” sequences involving multiple failures for more than the minimum set of equipment that could be available based on the success criteria. In other cases, it is not clear whether some “success” sequences are bounded by an analyzed “success” sequence. In addition, there are no T-H analyses performed to support the assumed success criteria of some mitigating systems and functions, such as the alternate containment cooling function. Please perform a systematic investigation to demonstrate the robustness of the assumed PRA success criteria for all “success” sequences of significant frequency.

---

**ANSWER:**

For alternate containment cooling by containment fan cooler units, the success criteria used in the PRA is one CCW pump and two containment fan cooler units. In order to provide the basis, MHI performed two MAAP analyses using calculation condition listed in Table 19.513-1. In Case 1 using two containment fan cooler units, although containment pressure rises after the initiating event, the pressure is decreased at approximately 13 hours due to heat removal via containment fan cooler units. On the other hand, containment pressure continues rising after initiating event in Case 2 using one containment fan cooler unit. The result shows that the one containment fan cooler unit will not remove heat in containment, resulting in failure of containment. For success criteria of CCW pump, since alternate containment cooling is effective mitigation system when heat removal via CS/RHR heat exchanger is unavailable, the CS/RHR heat exchanger with the highest heat load for CCWS is isolated by CCWS during alternate containment cooling by containment fan cooler units, which will not cause degradation of CCWS function nor cooling of other components. One containment fan cooler units requires water flow with approximately 100 m<sup>3</sup>/h. One CCW pump that has capacity of approximately

1000 m<sup>3</sup>/h can supply cooling water to all of four containment fan cooler units when the CS/RHR heat exchanger is isolated. Success criteria for alternate containment cooling using containment fan cooler units i.e., one CCW pump and two containment fan cooler units, are based on the above discussion. The MAAP analyses results will be documented in DCD Table 19.1-15.

DCD Table 19.1-16 summarizes the success criteria for each initiating event. MHI performed a systematic search to identify success sequences that do not have basis supported by T-H analysis results. Following is needed to provide basis using T-H analysis to support success criteria.

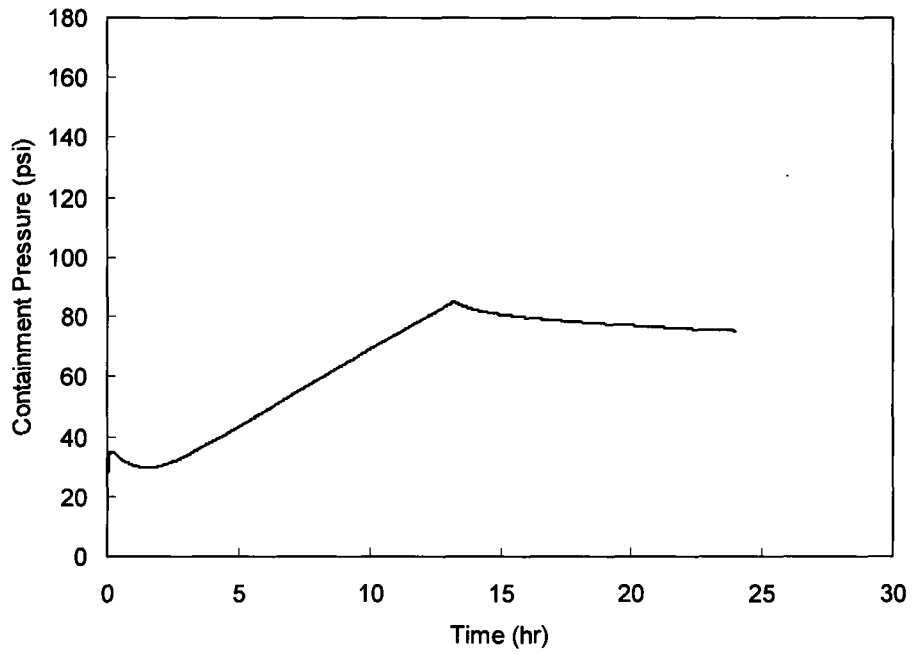
- (1) Core injection, decay heat removal and containment heat removal functions (MLOCA, SLOCA and VSLOCA events)  
Although 4 accumulators and 1 CS/RHR pump with 4 EFW pumps, 4 SGs and 3 MSDVs are success criteria in T-H analysis results in DCD Table 19.1-15 No 1.5, 2 accumulators and 1 CS/RHR pump with 3 EFW pumps, 3 SGs and 3 MSDVs are used in success criteria of PRA, which is based on Engineering judgment. This is because (1) number of accumulators has small impact on accident scenarios and (2) there is small difference in accident progress between 3 and 4 EFW pumps to SGs. The success criteria used in PRA are determined by engineering judgment and have no basis supported by T-H analysis.
- (2) Cool down and recirculation (SGTR event)  
Sequences #3, #4, #5 and #7, which are cool down and recirculation, have no basis supported by T-H analysis.
- (3) Sequence #20 in SGTR (No safety injection after isolation of ruptured SG)  
Sequence #20 does not provide T-H analysis results.

MHI will perform the T-H analyses to provide basis for the success criteria listed above by the end of this year and summarize the results in DCD Table 19.1-15.

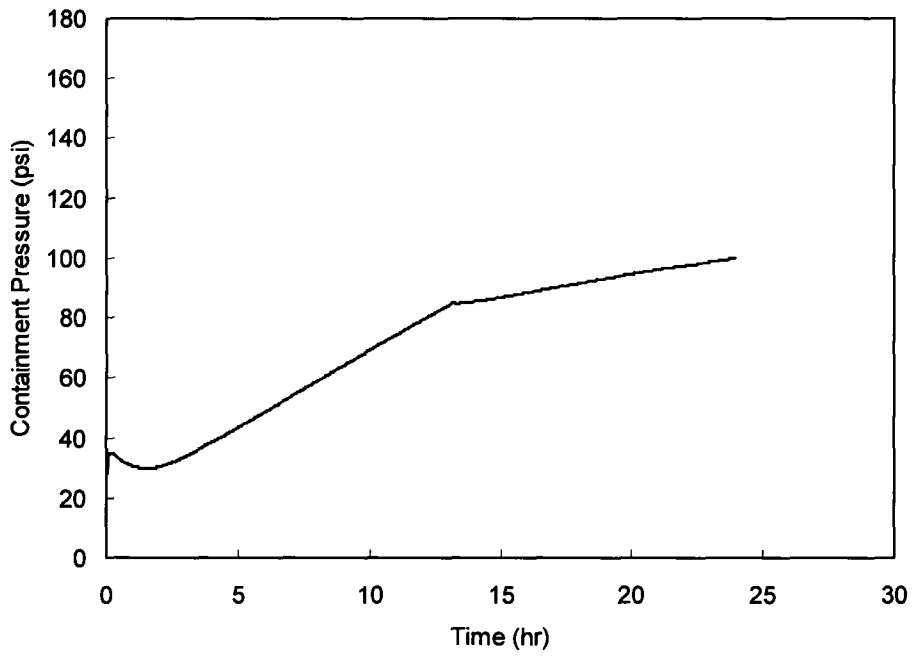
**Table 19-513-1 MAAP Analysis Condition for Alternate Containment Cooling**

Case	1	2
Initiating Event	LOCA with 8 inches break size	
High Head Injection	4/4	
Alternate Core Injection	0/4	
Accumulators	4/4	
Containment Spray	0/4	
Heat Exchanger	4/4	
Emergency Feedwater	4/4	
SG Secondary Side Cooling	0/4	
RCS Depressurization	Disable	
Containment Fan Cooler Units	2/4	1/4





**(1) Case 1 (Two Containment Fan Cooler Units)**



**(2) Case 2 (One Containment Fan Cooler Units)**

**Figure 19.513-1 Variation of The Containment Pressure**

Impact on DCD

Table 19.1-15 will be revised, as shown in attached mark-up.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

Table 19.1-15 Typical Results of Thermal/Hydraulic Analysis (Sheet 10 of 14)

No.	Objective of the analysis	Accident sequence description						Computer code and results	Insights from success criteria analysis
		Initiating event	SI pumps	Accumulators	EFW pumps	CS pumps	Other measures		
2.3		Hot leg 2 inch break	4	4	4	0	Alternate containment heat removal : 1 CS/RHR pump and 4 MSDVs at 30min	MAAP4.0.6 C/V pressure is at most about 40 psia < 216 psia	As discussed in the No.1.5 analysis, if SI pumps are not available, coolant injection into RV using CS/RHR must be effective even in small pipe break LOCA sequences. Therefore the alternate containment heat removal by coolant injection into RV is judged to be effective for any accident sequences.
2.4	To judge effectiveness of containment cooling using containment fan cooler units as alternate containment heat removal for LOCA	Hot leg 8 inch break	4	4	4	0	Alternate containment cooling : 2 containment fan cooler units after 30min at Pd	MAAP4.0.6 C/V pressure is at most about 75 psia < 216 psia and decreasing	The alternate measure using containment fan cooler system for alternate containment cooling is judged to be effective. However, the success criterion of containment fan cooler units is assumed that two containment fan cooler units are required for success  Note: Pd: Containment design Pressure
		Hot leg 8 inch break	4	4	4	0	Alternate containment cooling: 1 containment fan cooler unit after 30min at Pd	MAAP4.0.6 C/V pressure is at most about 100 psia < 216 psia and increasing	

INSERT

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-514**

In RAI Question 19-108 the staff requested more information regarding the basis for not having modeled in SGTR sequences an operator action to depressurize the RCS in order to equalize primary and secondary pressures and stop the leak after the ruptured SG is isolated. MHI responded that this operator action was assumed to be always successful because the operator has plenty of time to perform such an action. The staff followed up with RAI Question 19-366 requesting more detailed justification. In response, MHI included a top event (event DEP) in the SGTR event tree, which represents operator failure to equalize primary and secondary pressures, without any quantification. The staff review finds that event DEP is highly risk significant (e.g., risk achievement worth (RAW) value is about  $4 \times 10^{+3}$ ) and it is not obvious without the benefit of a T-H analysis that its contribution to risk (e.g., as measured by the Fussell-Vesely risk importance measure) is insignificant. Furthermore, if a cutoff probability of  $1 \times 10^{-5}$  is used for DEP, the sequence CDF would be  $4 \times 10^{-8}$  per year, which is comparable to the CDF of some of the reported dominant accident sequences. For these reasons, the failure probability of DEP must be estimated and documented together with all key assumptions and bases (e.g., T-H analysis) used in the estimation. In addition, event DEP should be addressed in the accident sequence quantification and importance analysis.

---

**ANSWER:**

As explained in the RAI responses, event heading "DEP" has high reliability because of redundancy of operator actions and sufficiently long allowable time for the actions. MHI will incorporate assumptions that core damage caused by failure to equalize the primary and secondary pressure hardly occurs due to redundancy of operator actions for equalization of the pressure and sufficiently long allowable time for the actions in the DCD Table 19.1-119. The basis is as follows:



## 1. Redundancy of Operator Actions

Any one of the following operator actions is sufficient to equalize the primary and secondary pressure.

- (1) Open safety depressurization valves
- (2) Start pressurizer auxiliary spray
- (3) Open depressurization valves for severe accident
- (4) Actuate pressurizer spray by re-starting RCPs

Since success of at least one can achieve equalization of the primary and secondary pressure, action for the equalization has redundancy. The above actions are considered in developing Emergency Response Guideline (ERG). Also, Items (1), (2) and (4) are considered in emergency operating procedures for Japanese operating PWR plants.

## 2. Sufficient allowable time

T-H analysis was performed to estimate allowable time for equalization of primary and secondary pressure. Table 19.514-1 lists the analysis condition, and Figure 19.514-1 shows the variation of leak rate from primary system to secondary system via the ruptured SG tube. The total leak volume after 24 hours from SGTR event is approximately 71,000 ft<sup>3</sup> (2000 m<sup>3</sup>). As described in DCD Section 6.3.2.2.3, since RWSP has allowable water with more than 81,230 ft<sup>3</sup> [2300 m<sup>3</sup>], operators have more than 24 hours for the actions. It is assumed that it will take an operator less than one hour to identify SGTR via secondary side radiation detectors. The allowable time enables the dependency among the above four actions to be negligible.

Failure probability of event heading "DEP" is estimated using the following assumptions.

- (1) Failure probability of each operator action is 1.0E-02
- (2) Dependency level among actions is zero dependency
- (3) Success criterion is one of four operator action

$$\begin{aligned} & \text{(Failure probability of DEP)} \\ & = (1.0E-02) \times (1.0E-02) \times (1.0E-02) \times (1.0E-02) \\ & = 1.0E-08 \end{aligned}$$

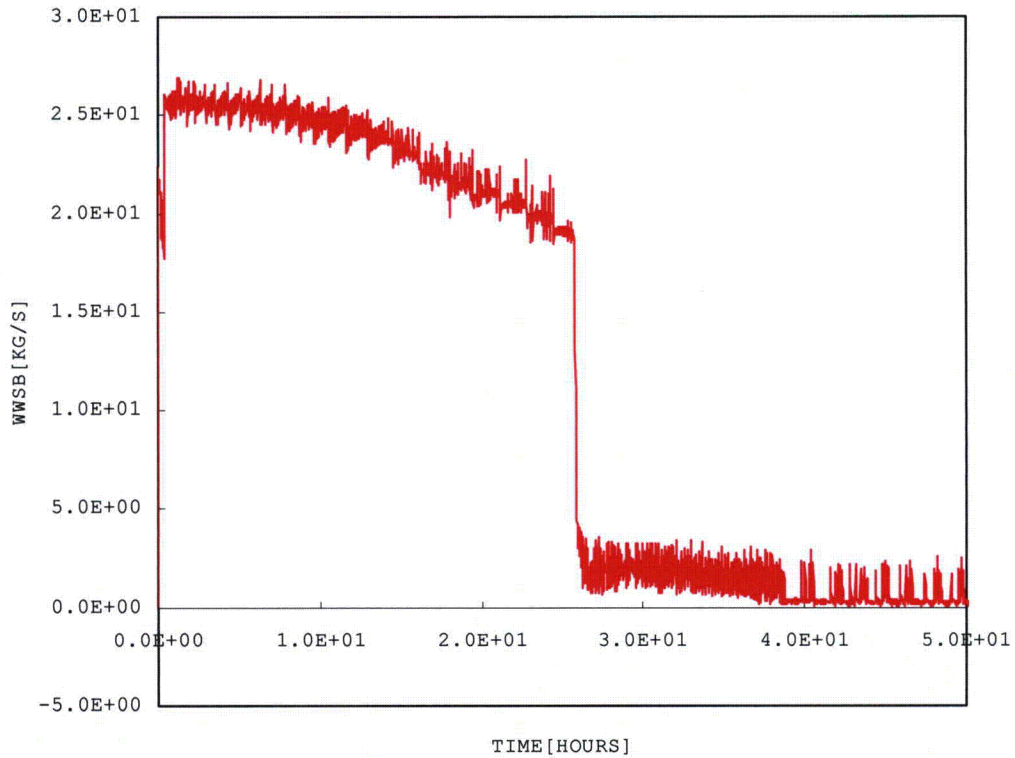
The failure probability of operator action to equalize the primary and secondary system is conservatively assumed to be 1.0E-05. Then,

$$\begin{aligned} & \text{CDF of SGTR Sequence \#2} \\ & = (\text{SGTR initiating event frequency}) \times (\text{Failure probability of DEP}) \\ & = (4.0E-03/\text{RY}) \times (1.0E-05) \\ & = 4.0E-08 \end{aligned}$$

Total CDF is estimated to be 1.1E-06/RY, which is 3.7% higher than of base case CDF. If failure probability of DEP is set to 0.0, CDF is equal to 1.0E-06/RY and FV importance 0.037. On the other hand, if the failure probability is set to 1.0, the CDF is estimated to be 4.0E-03/RY. Estimated RAW is equal to 4.0E+03 which exceeds the threshold to identify risk-significant basic event. The importance analysis results will be incorporated in DCD Chapter 19. The operator action to equalize RCS and secondary system will be documented in Table 19.1-119 as risk-significant human error.

**Table 19.514-1 Analysis Condition**

Parameters	Value
Initial RCS pressure	2250 psia
Initial RCS temperature	584 °F
Ruptured area of SG tube	4.81E-03 ft <sup>2</sup> (1 Tube Guillotine)
Exhaust condition	Atmosphere
Time for SI initiation after SGTR event	19min
Number of SI pumps	4
RWSP volume	81230 ft <sup>3</sup>



**Figure 19.514-1 Variation of Leak Rate from RCS through Ruptured SG Tube**

Impact on DCD

Table 19.1-119 will be also revised as shown in attached markup.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

**Table 19.1-119 Key Insights and Assumptions (Sheet 25 of 46)**

Key Insights and Assumptions	Dispositions
<p>36. Misalignment of remote-operated valves (e.g. motor-operated valves, air-operated valves), pumps and gas turbine generators after test and maintenance will be fixed before initiating events occur. Remote-operated valve open/close positions and control switch positions are monitored in the main control room, so they will be detected in a short time.</p>	<p>19.1.4 19.1.5 COL 13.5(5) COL 13.5(6)</p>
<p>37. The controls and displays available in the US-APWR control room are superior to conventional control room HSIs and, therefore, human error probabilities in the US-APWR operation would be less than those in conventional plants.</p>	<p>Chapter 18 19.1</p>
<p>38. In the SGTR event, operators perform at least one action to equalize primary and secondary pressure after the ruptured SG isolation.</p> <ul style="list-style-type: none"> <li>- Open safety depressurization valves</li> <li>- Start pressurizer auxiliary spray</li> <li>- Open depressurization valves for severe accident</li> <li>- Actuate pressurizer spray by restarting RCPs</li> </ul>	<p>19.2.5 COL 13.5(6) COL 19.3(6)</p>



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-515**

In RAI Questions 19-35 and 19-327 the staff requested additional information about I&C software failures modeled in the PRA, I&C hardware CCF, assumptions regarding diversity and their probabilities and associated uncertainties. MHI responded by performing sensitivity studies, including hardware CCF, and by re-classifying applications software failures into three groups. Groups 1 and 2 impact the safety-related performance and safety monitoring system (PSMS) while Group 3 impacts non-safety related I&C systems. This information was also included in Revision 2 of the DCD. The staff's review identified discrepancies between the provided event definitions and expected results, such as related cut sets (e.g., missing an expected cut set that includes the "transient" initiating event followed by I&C hardware CCF and failure of DAS with a frequency of  $1 \times 10^{-8}$  per year) and risk importance values (e.g., expected Group 1 software failure RAW value). The staff followed up with RAI Question 19-428 requesting clarification of the provided definitions of I&C hardware CCF and application software failures. Although in its response MHI provided more detailed information about the treatment of I&C hardware and software CCF in the system analysis, a more precise definition of these basic events is needed, in terms of what signals are impacted by each event.

---

**ANSWER:**

Definition of basic events regarding I&C system is as follows:

**Digital I&C hardware CCF (ID: SGNBTHWCCF)**

The digital I&C hardware CCF is defined as hardware failure within the PSMS which consists of RPS (reactor protection system), ESFAS (engineered safety feature actuation system) and SLS (safety logic system). Within the signals modeled in PRA, reactor trip and turbine trip signals are generated from RPS and other signals are generated from SLS through RPS and ESFAS. Then, under voltage signal to start AAC is excluded since it is designed to be diverse from the under voltage signal to start the emergency power source.

The hardware CCF results in no actuation of all automatic signals using PSMS. In addition, operators cannot monitor plant parameters using PSMS in the case of hardware CCF. PRA assumes failure probability of the hardware CCF with  $2.1E-06/\text{demand}$ .

#### **Digital I&C basic software CCF (ID: RTPBTSWCCF)**

Basic software CCF is defined as a failure of the MELTAC (Mitsubishi Electric Total Advanced Controller) operation system, which encompasses the common software for PSMS and plant control and monitoring system (PCMS). The basic software causes failure of all functions for signals and monitor of plant parameters using digital I&C system for PSMS and PCMS. PRA assumes failure probability of the basic software CCF with  $1.0E-07/\text{demand}$ .

#### **Application software CCF**

Application software of I&C system is different software for PSMS and PCMS. For PSMS, RPS consists of two separate digital controllers to achieve defense-in-depth through functional diversity, as described in DCD Section 7.2.1. Application software of PSMS is divided into two types in the PRA: one is Group 1 application software that detects SG water level sensor to generate EFW actuation signal. The other is Group 2 application software that detects sensors other than EFW water level sensor. These application software CCFs are represented as **SGNBTSWCCF1** and **SGNBTSWCCF2**, respectively. Application software for PCMS is represented as **SGNBTSWCCF3** in the US-APWR PRA. Group 1 application software CCF affects reactor trip, turbine trip, EFW actuation and EFW isolation signals. Group 2 application software CCF affects all safety-related signals other than EFW actuation and EFW isolation signals. Since both Groups 1 and 2 application software CCFs results in failure of reactor trip and turbine trip signals, reliability of these signals is higher than other signals. Group 2 application software is also applied to operator action to detect abnormal condition by safety-related sensors. Application software for PCMS is used for not automatic signal but only operator action to monitor non-safety related parameters such as containment pressure sensor (CSS-PI-014) or EFW water level sensor (EFS-LT-063, 073). PRA assumes that failure probabilities of PSMS and PCMS are  $1.0E-05/\text{demand}$  and  $1.0E-04/\text{demand}$ , respectively.

Table 19.515-1 shows the automatic signals considered in PRA, related I&C system and impact caused by signal failure. CCF of I&C system has impact on all initiating events other than reactor vessel rupture (RVR) event. US-APWR is designed to install DAS against I&C software CCF discussed above. DAS function is summarized in DCD Table 7.8-5, and Level 1 PRA expects the following functions:

- (1) Reactor Trip (Automatic)
- (2) Turbine Trip (Automatic)
- (3) Emergency Feedwater Actuation (Automatic)
- (4) Safety Injection Pump (Manual)
- (5) Safety Depressurization Valve (Manual)

Items (1) and (2) are effective functions to reduce risk caused by ATWS. Item (3) enables the reliability of decay heat removal system via SGs to be higher. Items (4) and (5) can also increase reliabilities of core injection system during LOCA event and feed and bleed operation.

Table 19.515-1 Signals In PRA and Impact Caused by Signal Failure (Updated Table 19.428-3)

#	FT Gate or Basic Event ID	Description	Hardware	Basic Software	Application Software		Impact Caused by Signal Failure	Related System	Related Initiating Event	Remarks
					G1	G2				
1	SGN-SA SGN-SB SGN-SC SGN-SD	ECCS actuation signal	X	X	NA	X	Failure to start SI pump	HHIS Feed and bleed operation	All initiating events, excepting, LOCCW, RVR and ATWS	DAS can be expected when I&C CCF occurs.
							Failure to start standby CCW pump	CCWS	All initiating events, excepting, LOCCW, RVR and ATWS	CCW pump start signal (#6) can be also expected.
							Failure to start standby essential chilled water pump	HVAC system	All initiating events, excepting, LLOCA, MLOCA, LOCCW and RVR	HVAC system failure has impact on operability of M/D EFW pump.
							Failure to open motor-operated valve to supply CCW to CS/RHR Hx	CS/RHR system	All initiating events, excepting, LOCCW, RVR and ATWS	
							Failure to start ESW pump	ESWS	All initiating events, excepting, LOCCW and RVR	
2	SGN-PA SGN-PB SGN-PC SGN-PD	Containment spray signal	X	X	NA	X	Failure to start CS/RHR pump	CS/RHR system	All initiating events, excepting, LOCCW, RVR and ATWS	Operator action can be also expected as recovery (A and C trains only).
							Failure to open containment spray injection line motor-operated valve	CS/RHR system	All initiating events, excepting, LOCCW, RVR and ATWS	Operator action can be also expected as recovery (A and C trains only).
							Failure to close CCW return and supply tie-line valve	CCWS	All initiating events, excepting, LOCCW, RVR and ATWS	Operator action can be also expected as recovery.
3	RTP-MF	Reactor trip	X	X	X	X	Failure of reactor trip	Reactor trip system	All initiating events, excepting LOCA, MLOCA, RVR, LOAC and LODC.	DAS can be expected when CCF of I&C system occurs. Reactor trip failure results in ATWS event.
4	TTP	Turbine trip	X	X	X	X	Failure of turbine trip	Turbine trip system	ATWS	DAS can be expected when CCF of I&C system occurs. Reactor trip failure results in core damage.
5	SGNST-CCWA SGNST-CCWB SGNST-CCWC SGNST-CCWD	Signal to open the normally closed motor-operated valve in the CCW line to provide CCW to the CS/RHR heat exchanger	X	X	NA	X	Failure to open motor-operated valve to supply CCW to CS/RHR Hx.	CS/RHRS (CCWS)	All initiating events, excepting LOCCW, RVR and ATWS	ECCS actuation signal (#1) can be also expected.
6	SGNST-CCWBPL SGNST-CCWDPL	Signal to start the standby CCW pump upon detection of low pressure at the CCW header	X	X	NA	X	Failure to start CCW pump	CCWS	All initiating events, excepting LOCCW, RVR and ATWS	ECCS actuation signal (#1) can be also expected.

#	FT Gate or Basic Event ID	Description	Hardware	Basic Software	Application Software		Impact Caused by Signal Failure	Related System	Related Initiating Event	Remarks
					G1	G2				
7	SGNST-BOA SGNST-BOB SGNST-BOC SGNST-BOD	Signal to start the Class 1E GTGs upon detection of under voltage of its associated Class 1E bus	X	X	NA	X	Failure to start Class 1E GTG	Emergency power supply system	All initiating events, excepting RVR and ATWS	This signal is required for loss of offsite power.
							Failure to separate RAT and connect UAT	Emergency power supply system	All initiating events, excepting RVR and ATWS	This signal is required for loss of offsite power.
8	SGNST-BOP1 SGNST-BOP2	Signal to start the AACs upon detection of under voltage of its associated non-Class 1E bus	Note	NA	Note		Failure to start AAC	Emergency power supply system	All initiating events, excepting RVR and ATWS	This signal is required for loss of offsite power.
							Failure to separate UAT and connect RAT	Emergency power supply system	All initiating events, excepting RVR and ATWS	This signal is required for loss of offsite power.
9	SGNST-ISA SGNST-ISB SGNST-ISC SGNST-ISD	Main steam isolation signal	X	X	NA	X	Failure to close main steam isolation valve	Main steam isolation system (Main steam suppression system)	SGTR	Operator action can be also expected as recovery.
10	SGNST-EFWPA SGNST-EFWPB SGNST-EFWPC SGNST-EFWPD	Signal to isolate EFW supplying to the faulted SG in SGTR event	X	X	X	NA	Failure to close EFW flow control valve or EFW isolation valve	EFWS	SGTR	
11	SGNST-ISA SGNST-ISB SGNST-ISC SGNST-ISD	Signal to open the turbine bypass valves in SGTR event	X	X	NA	X	Failure to close turbine bypass valves	Isolation of faulted SG (Main steam suppression system)	SGTR	Operator action can be also expected as recovery.
12	SGNST-ISA SGNST-ISB SGNST-ISC SGNST-ISD	Signals to open the main steam depressurization valve of the faulted loop in SGTR event	X	X	NA	X	Failure to close main steam depressurization valve of the faulted loop.	Isolation of faulted SG (Main steam suppression system)	SGTR	
13	SGNST-EFWPA SGNST-EFWPB SGNST-EFWPC SGNST-EFWPD	Signals to start EFW pumps	X	X	X	NA	Failure to generate EFW actuation signal	EFWS	All initiating events, excepting LLOCA, MLOCA and RVR	DAS can be expected when CCF of I&C system occurs.
14	SGNST-BOA SGNST-BOB SGNST-BOC SGNST-BOD	Signals to restart the CCW pumps in the loss of offsite power event	X	X	NA	X	Failure to re-start CCW pump in loss of offsite power event	CCWS	All initiating events, excepting LOCCW, RVR and ATWS	
							Failure to re-start ESW pump in loss of offsite power event	ESWS	All initiating events, excepting LOCCW, and RVR	

X: Applicable

NA: Not Applicable

Note: Common hardware, basic software and application software is not applied to signal to start AAC.

Impact on DCD

There is no impact on the DCD

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-516**

In RAI Question 19-275 the staff requested additional information regarding the basis for not including failure of HVAC in fault trees other than the fault tree developed for the motor-driven EFW pumps. In its response to RAI Question 19-275, MHI stated that HVAC operation has been considered in the PRA (Class 1E GTG area, ESF area (HHI and CS/RHR pumps), Class 1E electrical area (I&C, switchgear, batteries), main control room (MCR), and EFW pump area) but it was determined that the loss of HVAC has a significant impact only on the M-D EFW pumps for the following reasons:

- HVAC is not considered essential during the PRA mission time for T-D EFW pumps and GTGs due to design features
- HVAC in the ESF area, where HHI and CS/RHR pumps are located, is not modeled because analysis has shown that design limits will not be exceeded during the PRA mission time
- HVAC in the Class 1E electric area is not modeled due to its small contribution because it is running during normal operation and operator action, if necessary, to open doors and install temporary fans
- HVAC in the MCR is not modeled because of redundancy and the fact that operator actions can also be performed from the remote shutdown console (RSC) which has a diverse HVAC.

In its response to RAI Question 19-275, MHI also identified the following design and operational features in support of their modeling of HVAC in the PRA: (1) EFW T-D pumps are designed to operate for several hours without HVAC; (2) HVAC of the MCR and RSC are diverse; and (3) Operations, such as opening the doors and installation of temporary fans, will be performed in the event of loss of HVAC of the Class 1E electrical area. The staff followed up with RAI Question 19-383 requesting clarification of the statement that "the T-D EFW pumps are

designed to operate for several hours without HVAC” and more detailed information regarding the transfer of control from the MCR to the RSC. MHI responded that the time the T-D EFW pumps are required to operate during accidents is shorter than the time these pumps are designed to operate without HVAC cooling. However, the basis for this statement was not provided. Please provide a basis for this statement.

---

**ANSWER:**

MHI carried out the temperature analyses for each room. The analyses apply maximum temperature of normal condition listed in Table 9.4-1 of DCD Rev.3 as initial temperature in each room. Since temperature variation in each room strongly depends on initial temperature, assumed higher room temperature is much conservative condition.

Results of each temperature analysis are provided below.

**(1) T/D EFW Pump Room**

T/D EFW room temperature after 24 hours from loss of its HVAC system is less than 130°F, which does not exceed design temperature for T/D pump, 176°F. T/D EFW pump can operate within 24 hours without room cooling.

**(2) GTG Room**

Design feature of GTG adopted in US-APWR can be operable without HVAC system. HVAC system for GTG room is considered not essentially to maintain GTG function.

The GTG unit itself functions to intake outlet air to remove heat to the atmosphere, and the HVAC system is not shared with essential chilled water system which cools safety-related components such as SI pumps, CS/RHR pumps, T/D and M/D EFW pumps. If essential chilled water system fails due to the CCF, the failure has no impact on operability of GTG. The HVAC system failure for GTG has small impact on CDF due to independent HVAC system.

**(3) SI Pump Room**

SI pump room temperature after 24 hours from loss of its HVAC system is approximately 115°F, which is below design temperature for SI pump, 130°F. SI pump is operable within mission time without HVAC system.

**(4) CS/RHR Pump Room**

CS/RHR pump room temperature after 24 hours from loss of its HVAC system is approximately 110°F, which is less than design temperature for CS/RHR pump, 130°F. CS/RHR pump is operable within mission time without room cooling

**(5) Class 1E Electrical Area Room**

Using analysis condition considering installation of a temporary fan and opening door, Class 1E electrical room temperature after 24 hours from loss of its HVAC system is below 120°F, which does not exceed design temperature, 122°F. If operators do not install a temporary

fan and open door, the room temperature after 24 hours from loss of the HVAC system is above the design temperature. Therefore, operator actions, which are installation of a temporary fan and opening door, are important to maintain function in Class 1E electrical room.

Class 1E I&C room temperature, not considering installation of a temporary fan and opening door after 24 hours from loss of its HVAC system is approximately 120°F (49°C), which is not above design temperature, 122°F. Actions to install a temporary fan and open door following loss of HVAC system keeps Class 1E I&C room temperature below the analysis results. Mission time in the analysis is 24 hours in accordance with the time for frontline system. However, actuation signals such as ECCS actuation signal or containment spray signal are required within a short time after occurrence of an initiating event. Actual room temperature has sufficient margin, compared with the analysis results.

Class 1E battery room temperature, not considering installation of a temporary fan and opening door after 24 hours from loss of HVAC system is below 90°F, which is much less than design temperature 122°F. Class 1E battery room temperature can be kept below design temperature without operator actions.

**(6) MCR**

MCR temperature after 24 hours from loss of its HVAC system is 100°F. Since the action from MCR has redundancy, even if operator actions cannot be performed in MCR due to temperature increase, the action from the RCS can be implemented. The diversity has been described in DCD Subsection 7.4.1.5. The redundancy is design feature of US-APWR and has been listed in Table 19.1-119, Sheet 18 of the DCD Rev.3.

The design feature that safety-related equipment such as SI pumps, CS/RHR pumps and T/D EFW pumps can be operable without room cooling will be incorporated in DCD Table 19.1-119. Also, MHI performed sensitivity analysis assuming no restoration of HVAC system within mission time, resulting in no SI pumps, CS/RHR pumps, T/D and M/D EFW pumps. The resulting CDF is 3.8E-05/RV, which is approximately 40 times of the base case CDF. CCF of the HVAC system will result in failure of core injection system by SI pumps or CS/RHR pumps and secondary side cooling system via SGs. The US-APWR design that safety-related components such as SI pumps, CS/RHR pumps or EFW pumps can operate without room cooling within mission time is important to reduce CDF. A new table which summarizes the room temperature analysis results will be placed as the DCD Table 19.1-180 and be referenced in a disposition of each element in the DCD Table 19.1-119.

Impact on DCD

Table 19.1-119 will be revised and Table 19.1-180 will be inserted as shown in attached markup.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

Table 19.1-119 Key Insights and Assumptions (Sheet 1 of 46)

Key Insights and Assumptions	Dispositions
<b>Design features and insights</b>	
1. High Head Safety Injection System	
- The high head safety injection system consists of four independent and dedicated SI pump trains.	6.3.2.1.1
- The SI pump trains are automatically initiated by ECCS actuation signal, and supply borated water from the RWSP to the reactor vessel via direct vessel injection line.	6.3.2.1.1
- Each SI pump is connected to a dedicated direct vessel injection nozzle for injection into the reactor downcomer region.	6.3.2.1.1
- SI pump suction isolation valves (SIS-MOV-001A/B/C/D) remain open during normal and emergency operations. These valves are remotely closed by operator action from MCR or RSC to isolate RWSP to terminate leak or if pump/valve maintenance requires it.	6.3.2.2.6.1
- This system provides the safety injection function during LOCA events and feed and bleed operation.	6.3.3 19.2.5 COL13.5(6) COL19.3(6)
- During plant shutdown, safety injection provides RCS makeup function in loss of RHRs. In the case of failure of operable SI pump, the pumps that are locked out for LTOP compliance can be used if available.	5.2.2.1.2 5.2.2.2.2 19.2.5 COL13.5(6) COL19.3(6)
- SI pump can be manually actuated by DAS from MCR.	7.8.1.1.1 Table 7.8-5
- SI pumps are operable regardless of HVAC system of the safeguard component area within mission time.	Table 19.1-180



**Table 19.1-119 Key Insights and Assumptions (Sheet 5 of 46)**

Key Insights and Assumptions	Dispositions
<ul style="list-style-type: none"> <li>- The RHR system is used to provide core cooling when the RCS must be partially drained to allow maintenance or inspection of the reactor head, SGs, or reactor coolant pump seals.</li> </ul>	5.4.7.2.3.6
<ul style="list-style-type: none"> <li>- When the RCS temperature and pressure are reduced to 350°F and 400 psig, the RHRS provides the heat removal function.</li> </ul>	5.4.7.2.3.3 19.1.6
<ul style="list-style-type: none"> <li>- During mid-loop operation, low-pressure letdown line isolation valves, which are air-operated valves, are automatically closed to isolate CVCS from RHRS by detection of RCS loop low-level signal. This interlock is useful to prevent loss of reactor coolant inventory.</li> </ul>	5.4.7.2.2.3 5.4.7.2.3.6 7.6.1.7 TS 3.4.8 TS 3.9.6
<ul style="list-style-type: none"> <li>- The containment spray/residual heat removal pump full-flow test line stop valves (RHS-MOV-025A/B/C/D) are locked closed.</li> </ul>	5.4.7.2.2.3

- CS/RHR pumps are operable regardless of HVAC system of the safeguard component area within mission time. Table 19.1-180

Table 19.1-119 Key Insights and Assumptions (Sheet 11 of 46)

Key Insights and Assumptions	Dispositions
<ul style="list-style-type: none"> <li>- The EFWS is automatically initiated by EFW actuation signal or by DAS.</li> </ul>	7.3.1.5.9 7.8.1.2.2 Table 7.8-5 10.4.9.1
<ul style="list-style-type: none"> <li>- The EFWS design is provided with the capability to automatically terminate EFW flow to a depressurized (faulty) SG and to automatically provide EFW to the intact SGs.</li> </ul>	7.2.1.5.10 10.4.9.1 10.4.9.2 10.4.9.2.1
<ul style="list-style-type: none"> <li>- The system supplies feedwater to the SGs at a sufficient flow rate to meet the requirements for the transient conditions or postulated accidents and hot standby.</li> </ul>	10.4.9
<ul style="list-style-type: none"> <li>- Motor-driven EFW pumps require room cooling for operation. On the other hand, turbine-driven EFW pumps are operable regardless of <del>the availability of</del> room cooling.</li> </ul>	<div style="border: 1px solid red; padding: 2px;">Table 19.1-180</div>

Table 19.1-119 Key Insights and Assumptions (Sheet 16 of 46)

Key Insights and Assumptions	Dispositions
- A-AAC GTG operates automatically by the undervoltage relays on bus P1 and B-AAC GTG operates automatically by the bus undervoltage relays on bus P2 during the LOOP condition. The time is less than 100 seconds after receiving the signal.	8.3.1.1.1 8.3.1.1.3 8.3.1.1.3.1
- The rooms for the A-AAC GTG and B-AAC GTG are physically separated from each other and also from the Class 1E GTG rooms.	8.3.1.1.1
- Normal preferred offsite power is provided from the RATs and the alternate preferred offsite power is provided from the UATs.	8.3.1.1.2.1
- During all modes of plant operation including normal and emergency shutdown, and accident conditions, Class 1E 6.9kV ac buses A and B trains and C and D trains are normally powered from the RAT3 and RAT4, respectively. On the other	8.3.1.1 8.3.1.1.1 8.3.1.1.2 8.3.1.1.2.4
GTG can operate regardless of the loss of HVAC case caused by the essential chilled water system.	Table 19.1-180
- Glass 1E GTGs are automatically started by signals such as ECCS actuation signal, under-voltage signal on Class 1E 6.9kV.	8.3.1.1.2.3 8.3.1.1.3.1
- The AAC GTG is started automatically and the incoming breakers from the offsite power supply to 6.9kV permanent bus are tripped by the under-voltage signal on the permanent bus.	8.4.1.3
15. RCP seal	
- RCP seal can keep its integrity for at least one hour without water cooling.	8.4.2.1.2
- If loss of seal injection should occur, CCW continues to provide flow to the thermal barrier heat exchanger; which cools the reactor coolant. The pump is able to maintain safe operating temperatures and operate safely long enough for safe shutdown of the pump.	5.4.1.3.3
- If loss of CCW should occur, seal injection flow continues to be provided to the RCP. The pump is designed so that the seal injection flow is sufficient to prevent damage to the seals with a loss of thermal barrier cooling.	5.4.1.3.4



Table 19.1-119 Key Insights and Assumptions (Sheet 18 of 46)

Key Insights and Assumptions	Dispositions
<p>17. Essential Chilled Water System</p> <ul style="list-style-type: none"> <li>- The essential chilled water system consists of four independent trains and includes a water-cooled chiller, a chilled water pump, and a compression tank.</li> <li>- Upon receipt of ECCS actuation signal, the operating essential chillers and pump continues to run and the standby essential chillers and pumps start.</li> <li>- The system provides HVAC system to each room such as EFW pump area.</li> <li>- The operator has the same functional control and monitoring capability at the RSR as in the MCR. The RSC provides equivalent functions of the operational VDUs and the safety VDUs in the MCR. The transfer of control to the RSR has no affect on any non-safety or safety-related control functions, including automatic load sequencing to accommodate LOOP. The operator has complete capability to control all manual and automatic modes. Adequate emergency lighting is provided on the pathways from the MCR to the RSR and to accommodate local effluent sampling.</li> <li>- Operators open the doors or install temporary fans to prevent room temperature rising in the loss of HVAC for Class 1E electric room.</li> </ul>	<p>9.2.7.2.1 9.2.7.2.1.1</p> <p>9.2.7.2.1</p> <p>9.2.7</p> <p>7.4.1.5</p> <p>Table 19.1-180</p>

**Table 19.1-180 Room Temperature Analysis Results for Each Area**

Area	Temporary Fan	Door	Initial Temperature [F] <small>Note</small>	Results and Remarks
GTG Room	-	-	-	GTG has independent HVAC system from essential chilled water system
T/D EFW Pump Room	Not installed	Close	105	Not exceed the design limit
SI Pump Room	Not installed	Close	105	Not exceed the design limit
CS/RHR Pump Room	Not installed	Close	105	Not exceed the design limit
Class 1E Electrical Area Room	Not installed	Close	95	Exceed the design limit temperature and operator actions such as installation of a temporary fan and opening door are effective not to exceed the design limit temperature
	Installed	Open		Not exceed the design limit
Class 1E I&C Room	Not installed	Close	79	Not exceed the design limit
Class 1E battery Room	Not installed	Close	77	Not exceed the design limit
Main Control Room	Not installed	Close	78	Possibility to exceed the design limit Operators can also perform similar actions from RSC



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-517**

In RAI Questions 19-200 and 19-381, the staff requested clarification regarding the assumption of “different crews” made in evaluating the dependency level among human errors in SGTR sequences, such as the dependency among operator failure to close the MSIV associated with a faulted SG, the operator failure to isolate a faulted TBV and the operator failure to depressurize the primary using the SDVs. In its responses, MHI stated that “different” and “same” crews are defined based on the location where the operator action is performed. However, it appears that the same crew is performing the cognition aspects for all these actions from the control room and, therefore, the assumption of “different” crews is not valid. Please perform a systematic search of all significant accident sequences in the PRA to ensure that dependencies among operator errors are properly assessed.

---

**ANSWER:**

For the operator actions requested in this RAI Question, operator failures to close the MSIV associated with a faulted SG and to depressurize the primary system using the SDVs are implemented in the main control room (MCR). On the other hand, isolation of faulted TBV is local action. US-APWR PRA assumed the different crews among these human errors. However, cognition aspects for these actions are performed in the MCR by same operators and the assumption regarding Crew will be changed to “same” and re-estimation will be implemented.

For other human errors, dependency levels among the human errors are re-estimated using Table 9.4.3-1 of US-APWR PRA Report (MUAP-07030, Proprietary) and Figure 19.517-1. The table summarizes assumptions to estimate dependency level among human errors considered in the PRA. Dependency level among human errors is estimated by four factors, which are Crew, Time, Location and Cue. US-APWR PRA uses the following basis to estimate the factors.

- Crew

For all human actions, operators detect the abnormal condition in the MCR. Assumption "same crew" is applied to all human actions in the US-APWR PRA.

- Time

NUREG/CR-6883 provides the basis to estimate the factor, which is from within seconds to a few minutes. Allowable time among operator actions considered in US-APWR is more than a few minutes. For example, operator actions for alternate charging pump cooling by fire protection water supply system (Basic Event ID: **ACWOO02FS**) or non-essential chilled water system (Basic Event ID: **ACWOO02CT**) has one hour since RCP seal integrity can be maintained for one hour with no seal injection. Operator action for alternate containment cooling by containment fan cooler units (Basic Event ID: **NCCOO02CCW**) has also sufficient allowable time with more than 10 hours. Assumption "Not close" is applied to all human actions in the US-APWR PRA.

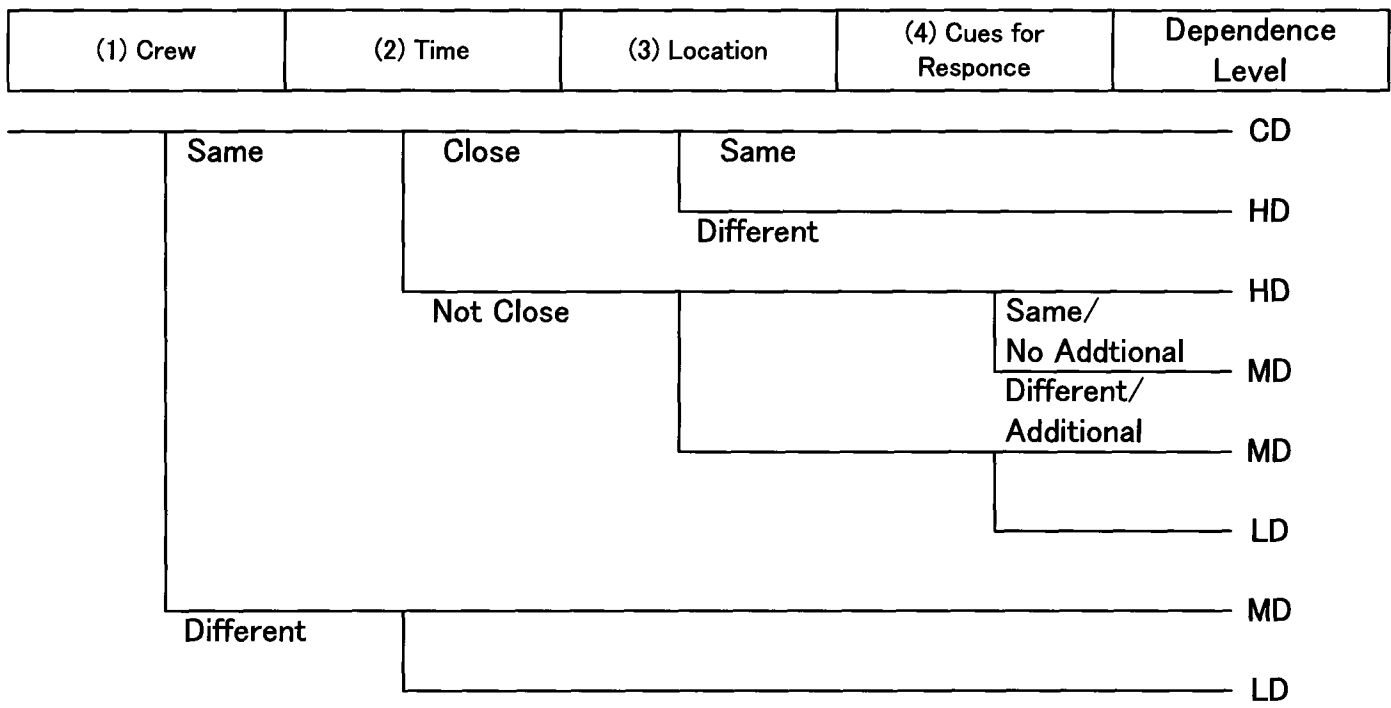
- Location

As answered in the RAI #369-2625 Question 19-340, operators actions will be performed using different panel. In the operational visual display unit (VDU) of US-APWR, the layout of controllers & monitoring alignment in each window are different and this feature would make the operator perceive them as different locations.

- Cues for response

Based on NUREG/CR-6883, additional cues can be applied if there is a specific procedural callout or a different procedures, or additional alarm(s) or display exists. Cues are assumed to be "Different/Additional" in the current estimation and will be changed to "Same/No additional" because of no sufficient basis to assume "Different/Additional".

To reflect the above discussion, the CDF is re-estimated to be 1.1E-06/RV, which is 3% higher than the base case CDF reported in DCD Rev. 3.



Notes; If this error is 3rd error in the sequence, then the dependency level is at least moderate, if this error is 4th error in the sequence, then the dependency level is at least high, and if this error is more in the sequence, then the dependency level is complete.

**Figure 19.517-1 Decision Tree to Determine the Dependency Level between Multiple Human Failure Events (Same as DCD Figure 19.1-3)**

Impact on DCD

There is no impact on the DCD

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

Dependency level among human errors will be updated to reflect the response to this RAI.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-518**

In RAI 19-287, the staff requested additional information regarding the screening criteria of external hazards. Although MHI discusses criteria for screening out external hazards from detailed risk assessment, the specific analysis (PRA or bounding) of the capability of the US-APWR design to withstand site-specific external hazards other than earthquakes (e.g., external flooding and high winds) was left to be performed by the COL applicant referencing the US-APWR design. The COL Action Item 19.3(4), included in Revision 2 of the DCD, requires COL applicants referencing the US-APWR design to assess site specific information and associated external events (high winds and tornadoes, external floods, transportation, and nearby facility accidents). Please clarify this COL action item in the DCD to state that all site-specific external hazards must be addressed by screening or analysis and not just those listed in parenthesis.

---

**ANSWER:**

COL action item COL 19.3(4) will be revised as follows.

COL 19.3(4) The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and all associated *potential* site-specific external *hazards (both natural and man-made hazards) that may affect the facility are screened out or subjected to analysis.*

Impact on DCD

COL Item 19.3(4) will be revised, as shown attached mark-up.

Impact on R-COLA



COL Item 19.3(4) in Table 1.8-201 will be revised, shown in attached markup.

Impact on S-COLA

COL Item 19.3(4) in Table 1.8-201 will be revised, shown in attached markup.

Impact on PRA

There is no impact on the PRA.

---

**19.3 Open, Confirmatory, and COL Action Items Identified as Unresolved**

The following subsections identify the open, confirmatory and COL action items associated with this Chapter.

**19.3.1 Resolution of Open Items**

There are no open items associated with this Chapter.

**19.3.2 Resolution of Confirmatory Items**

There are no confirmatory items associated with this Chapter.

**19.3.3 Resolution of COL Action Items**

The following are the COL action items associated with this Chapter:

COL 19.3(1) The COL Applicant who intends to implement risk-managed technical specifications continues to update Probabilistic Risk Assessment and Severe Accident Evaluation to provide PRA input for risk-managed technical specifications. Peer reviews for the updated PRA will be performed prior to the use of PRA to risk-informed applications.

COL 19.3(2) Deleted

COL 19.3(3) Deleted

COL 19.3(4) ~~The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and associated site specific external events (high winds and tornadoes, external floods, transportation, and nearby facility accidents).~~

COL 19.3(5) Deleted

COL 19.3(6) The COL Applicant develops an accident management program which includes severe accident management procedures that capture important operator actions. Training requirements are also included as part of the accident management program.

The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and all associated potential site-specific external hazards (both natural and man-made hazards) that may affect the facility are screened out or subjected to analysis.

**Comanche Peak Nuclear Power Plant, Units 3 & 4  
COL Application  
Part 2, FSAR**

CP COL 1.8(2)

**Table 1.8-201 (Sheet 61 of 62)**

**Resolution of Combined License Items for Chapters 1 - 19**

COL Item No.	COL Item	FSAR Location	Resolution Category
COL 19.3(1)	The COL Applicant who intends to implement risk-managed technical specifications continues to update Probabilistic Risk Assessment and Severe Accident Evaluation to provide PRA input for risk-managed technical specifications.	19.1.7.6	4
COL 19.3(2)	Deleted from the DCD.		
COL 19.3(3)	Deleted from the DCD.		
COL 19.3(4)	<del>The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and associated site specific external events (high winds and tornadoes, external floods, transportation, and nearby facility accidents).</del>	<del>19.1.1.2.1</del> <del>19.1.4.1.2</del> <del>19.1.4.2.2</del> <del>19.1.5</del> <del>19.1.5.2.2</del> <del>19.1.5.3.2</del> <del>19.1.6.2</del> <del>19.2.6.1</del> <del>19.2.6.1.1</del> <del>19.2.6.2</del> <del>19.2.6.4</del> <del>19.2.6.5</del> <del>19.2.6.6</del> Table 19.1-201 Table 19.1-202 Table 19.1-203 Table 19.2-9R Figure 19.1-201	3a
	<b>The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and associated all potential site-specific external hazards (both natural and man-made hazards) that may affect the facility are screened out or subjected to analysis.</b>		
COL 19.3(5)	Deleted from the DCD.		

19-518-3



**Table 1.8-201 Resolution of Combined License Items for Chapters 1–19**

COL Item No.	COL Item	FSAR Section	Resolution Category
COL 18.10(2)	Deleted from the DCD.		
COL 18.11(1)	Deleted from the DCD.		
COL 18.11(2)	Deleted from the DCD.		
COL 18.12(1)	Deleted from the DCD.		
COL 19.3(1)	The COL Applicant who intends to implement risk-managed technical specifications continues to update Probabilistic Risk Assessment and Severe Accident Evaluation to provide PRA input for risk-managed technical specifications.	19.1.7.6	NA
COL 19.3(2)	Deleted from the DCD.		
COL 19.3(3)	Deleted from the DCD.		
COL 19.3(4)	<del>The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and associated site-specific external events (high winds and tornadoes, external floods, transportation, and nearby facility accidents).</del>	19.1 19.2	3a
COL 19.3(5)	The Probabilistic Risk Assessment and Severe Accident Evaluation is updated as necessary to assess specific site information and associated all potential site-specific external hazards (both natural and man-made hazards) that may affect the facility are screened out or subjected to analysis.		2
COL 19.3(6)		program.	

19-518-4

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

06/30/2011

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No.52-021**

**RAI NO.:** NO. 750-5675 REVISION 2  
**SRP SECTION:** 19 – Probabilistic Risk Assessment and Severe Accident Evaluation  
**APPLICATION SECTION:** 19  
**DATE OF RAI ISSUE:** 04/28/2011

---

**QUESTION NO. : 19-519**

In RAI Questions 19-290 and 19-389, the staff requested additional information and clarification regarding missing dominant mixed cut sets containing random failure probability higher than  $1.0 \times 10^{-3}$  in the PRA-based SMA results. Specifically, the staff requested an explanation regarding missing mixed cutsets comprised of random common cause failure (CCF) of gas turbine generators (GTGs) to start and run and seismic failure of the switchyard ceramic insulators (HCLPF of 0.08g pga). These mixed cut sets lead to station blackout with no recovery possible since no credit is taken in the PRA-based SMA for the non-safety grade alternate ac gas turbine generators. In its response MHI stated that the above described mixed cutsets have been screened out because the failure probability of the random event (i.e., unavailability of all GTGs) is lower than the cutoff value of  $1.0 \times 10^{-3}$ . The staff notes that the probability of random failure of the GTGs to start and run for their entire mission time (assumed to be 24 hours in the US-APWR PRA) is higher than the cutoff value of  $1.0 \times 10^{-3}$  when all failure modes and the entire mission time are considered. Please address in the DCD the mixed cutset resulting from a seismically-induced LOOP and the random CCF of the GTGs together with a discussion of the resulting risk, as necessary.

---

**ANSWER:**

Cut-off value to estimate mixed cutsets is 1.0E-15. US-APWR PRA Report (MUAP-07030, Proprietary) Subsection 24.4.10.5.2 provides the mixed cutsets of basic events with failure probability of greater than 1.0E-03.

DCD Revision 3 page 19.1-88 provides the following statement

“The probability that all gas-turbine generators (GTGs) fail to run for 24 hours is 1.15E-3. But, the mixed-cutsets of all GTGs failure are not involved because the failure modes of GTGs are classified in failure of run for first hour (1.6E-4) and failure of run for remaining 23 hours (9.9E-4) in the PRA model.”

The below is a mixed cutsets of random CCF of Class 1E GTG (all failure mode) with seismically-induced LOOP

- Combination 5:  
Seismically induced loss of offsite power initiating event  
[AND] Class-1E Gas Turbine Generators A,B,C and D CCF (all failure modes)

The mixed cutset does not include the failure of alternate GTGs (i.e., AAC) since no credit is taken in the PRA-based SMA for the non-safety grade AAC. Practical mixed cutsets which result in station blackout will include the cutsets of AACs because the HCLPF value or random failure probabilities of AACs will be more higher than the lowest HCLPF value (0.08g pga) of loss of offsite power (the switchyard ceramic insulators).

Even if it is assumed that the mixed cutsets of the Combination 5 leads to station blackout, the frequency will be less than 1.0E-06 per year. The basis is as follows:

- The seismic exceedance frequency greater than 0.08 g pga will be less than approximately 1.0E-02 per year reported in NUREG-CR 6607 "Guidance for Performing Probabilistic Seismic Hazard Analysis for a Nuclear Plant Site: Example Application to the Southeastern United States".
- Mean failure probability of HCLPF is approximately 0.01
- Unavailability of all Class 1E GTGs is approximately 1.0E-03

Probability of the cutsets can be estimated to be less than 1.0E-06 per year ( $1.0E-02$  per year  $\times$   $0.01 \times 1.0E-03$ ). The practical probability of station blackout caused by seismic will be reduced due to the consideration of AACs.

#### Impact on DCD

DCD Subsection 19.1.5.1.2 will be revised as shown in attached mark-up

#### Impact on R-COLA

There is no impact on the R-COLA.

#### Impact on S-COLA

There is no impact on the S-COLA.

#### Impact on PRA

There is no impact on the PRA.



- Combination 2:

Seismically induced small LOCA initiating event

[AND] Seismically induced failure of turbine driven EFW pumps  
(including supporting system failure)

[AND] Random failure of one motor driven EFW pump  
(including supporting system failure)

- Combination 3:

Seismically induced loss of offsite power initiating event

[AND] Seismically induced failure of motor driven EFW pumps  
(including supporting system failure)

[AND] Random failure of one turbine driven EFW pump  
(including supporting system failure)

The probability that all gas-turbine generators (GTGs) fail to run for 24 hours is  $1.15E-3$  which is sum of the mixed cutsets of failure of run for first hour ( $1.6E-4$ ) and failure of run for remaining 23 hours ( $9.9E-4$ ) in the PRA model. The mixed cutset of loss of offsite power and all failure modes of Class 1E GTG CCF is as follows. This mixed cutset does not include the cutset related to AACs conservatively.

- Combination 5:

Seismically induced loss of offsite power initiating event

[AND] Class-1E Gas Turbine Generators A,B,C and D CCF (all failure modes)

[AND] Random failure of one motor driven EFW Pump

(including supporting system failure)

~~The probability that all gas-turbine generators (GTGs) fail to run for 24 hours is  $1.15E-3$ . But the mixed cutsets of all GTGs failure are not involved because the failure modes of GTGs are classified in failure of run for first hour ( $1.6E-4$ ) and failure of run for remaining 23 hours ( $9.9E-4$ ) in the PRA model.~~

Multiple failures of SSCs are required in order to drive the plant to core damage. The probability of this scenario would be low. From these results, random failures are concluded to not have significant impact on seismic safety.

One of the objectives of a seismic event is to identify vulnerabilities of containment functions. These include containment integrity, containment isolation and prevention of bypass functions. Seismic capacities for these functions are as follows.